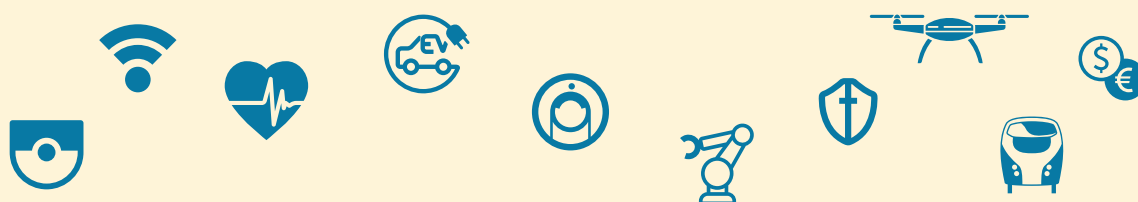


Prepare for Billions

The IoT 2020 IT Infrastructure Readiness Indicator



An IDC Thought
Leadership White Paper

Sponsored by:



**Hewlett Packard
Enterprise**

Executive Summary

The Internet of Things (IoT) continues to fundamentally transform economies worldwide. Thanks to the era of “connecting the unconnected,” cities, transportation, supply chains, commercial real estate, and industries like health care, retail, and entertainment are becoming smarter, more efficient, and more resilient. An IoT strategy for any organization should, holistically speaking, be part of a bigger Digital Transformation (DX) vision. Digital Transformation — the application of a technology-centric business vision and accompanying strategies — is mandatory for firms to thrive in a digital economy. Firms embark on DX to create value and extend their competitive advantages through new products and services, new business models and relationships, improve customer experience, and increase operational efficiencies.

IDC believes that despite massive investment in IoT, much of the impact of this transformation is yet to be felt. In fact, IDC estimates that the worldwide count of IoT devices in operational deployments will reach 28.1 billion by 2020, growing at a CAGR of 17.5% between 2016 and 2020. The world will feel the true impact of the IoT era as new IoT deployments go into production powered by a new breed of applications and workloads that are distributed to the edge to harness and analyze data from every connected device in a timely fashion. Much of this growth hinges on the ability of firms to transform their IT infrastructure and operations as a part of IoT readiness initiatives.

Many firms have been preparing for the IoT wave. IDC recently conducted a study (see Methodology, page 4, for details) that shows that more than half of firms worldwide have a forward-looking IoT strategy. This strategy underpins their quest to articulate competitive differentiation in the market, seek greater efficiencies in how they operate, and target superior customer experiences by improving their products and services. In fact, a full 60% of surveyed firms rate their own IoT strategy to be highly mature.

While much has been documented on IoT and its transformative effects on firms and industries, there is little documentation on how to approach IT infrastructure readiness. By analyzing the results of a recent study, IDC has produced an [IoT IT Infrastructure Readiness Index](#) (referred throughout this paper as the Index). The Index places firms into four categories based on their level of IoT IT readiness. Note that the Index seeks to measure IoT IT infrastructure readiness and not firms’ willingness to adopt IoT (the two being markedly different cases). The four categories referred to in this paper and in the Index, are: [IoT Amateurs \(IT is unready for IoT growth\)](#), [IoT Rookies \(IT is minimally ready for IoT growth\)](#), [IoT Pros \(IT is nearly ready for IoT growth\)](#), and [IoT All-Stars \(IT is ready for IoT growth\)](#). IDC found that only 16% of firms qualify as IoT All-Stars. The Index provides firms guidance on moving to a state of higher readiness.

IDC uses four “spokes” or technology areas to assess, measure, and prescribe IoT IT Infrastructure readiness (regardless of whether this infrastructure belongs to corporate IT, line-of-business IT, or Operations Technology): (1) **Cloud-first Delivery Model**, (2) **Advanced Analytics and Insight**, (3) **Data Flow and Action Control**, and (4) **Data Governance, Risk Management, and Compliance (GRC)**. In this paper, we examine each of these areas to describe the differences between firms at various stages of IoT IT readiness. At a high level, the firms in these readiness categories are differentiated by three key aspects:

■ **Attitude toward IoT**

Low IoT IT readiness firms focus upon efficiency, while often viewing IoT as a chore and a risk to the business. They would prefer to avoid IoT initiatives, taking them on only when they have no choice.

High IoT IT ready firms, on the other hand, see IoT as an opportunity to transform their businesses. These firms are more ambitious with their IoT initiatives and tend to be frustrated by technology limitations that slow them down or hold them back.

■ **Moving from data-centric to action-centric IoT**

Low IoT IT readiness firms are highly likely to use IoT in a “data-centric” way, meaning their IoT devices are one-way sensors, pure data sources that do not act as change agents for the corporations that deploy them. Such firms are considerably less likely to use the advanced technologies necessary for taking direct action using these IoT devices but rather to use them only to inform their own internal business operations.

High IoT IT readiness firms, on the other hand, are likely to employ “action-centric” IoT devices. These devices are active change agents that not only carry out all the functions of “data-centric” IoT but additionally can respond to or act based on specific circumstances. Such firms make much more use of the advanced technologies and business processes that facilitate and automate these activities in real time or near real time.

■ **Readiness in technology adoption**

High IoT IT readiness firms employ diverse types of IT infrastructure technology that directly influence or are influenced by the IoT strategy. They have a greater propensity to leverage advanced network technologies, invest in advanced IT infrastructure provisioning and management frameworks, and develop custom next-generation applications in aid of their IoT strategies. Such firms (to the extent they are allowed by industry regulations) make informed use of on- and off-premises cloud types and tiers for efficient data capture, analysis, and insight.

Low IoT IT readiness firms tend to be more reactive in their use of IT and are slower to embrace new frameworks and delivery models.

Firms seeking to advance their IoT IT infrastructure readiness should assess the design of their IT infrastructure. They could take a clean-slate approach to building a modern IT infrastructure or, a retrofit upgrade of existing infrastructure. In either case, the goal of IT infrastructure should be agility, flexibility, and scalability to support of strategic IoT-centric business outcomes such as timely insight from diverse and disparate data sources. These accelerated insights can drive time-to-revenue, shorten design cycles, and improve response times. In the same vein, IT infrastructure upgrades that enable a shift to higher levels of IoT readiness ought to be treated as strategic activities as opposed to a chore to be taken on reactively.



Methodology

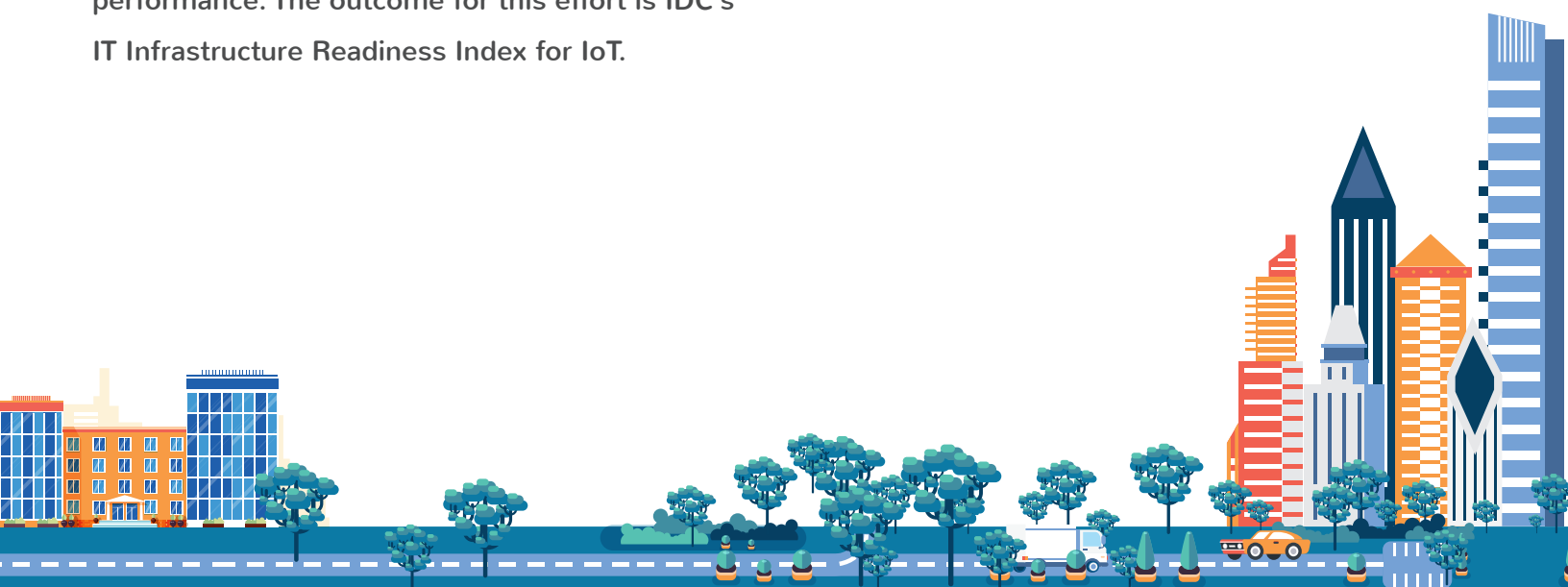
IDC recently conducted a study among both corporate IT and line-of-business (LOB) executives from more than 600 firms with 500 employees or more. To participate, such firms needed either an IoT strategy in place today or specific plans to deploy one within the next 12 months. The study enabled IDC to measure firms' current state of readiness and determine their attitudes and actions toward IoT to place their overall IoT strategy in context. By correlating responses to actual performance on key metrics, IDC could determine the IoT behaviors that correspond to business success. Using these behaviors as a guide, IDC grouped all respondents into the four categories of IoT IT readiness (in order from least ready to most): IoT Amateurs, IoT Rookies, IoT Pros, and IoT All-Stars. IDC went on to measure these groups' overall behavior to discover differences between leaders and laggards in IoT performance. The outcome for this effort is IDC's IT Infrastructure Readiness Index for IoT.

Notes on Terminology

Core refers to the core datacenter. For example, **analytics at the core** refers to analytics that occur inside the core datacenter, rather than at the edge, which lies the outside the datacenter.

Cloud refers to a cloud delivery model for infrastructure. It incorporates on- or off-premises cloud infrastructure and (to the extent they are allowed by industry regulations), public cloud services.

IoT IT and IoT IT infrastructure are used interchangeably in this paper



IoT IT Infrastructure Readiness Levels

Table 1 illustrates the four IoT IT readiness categories. They are:

IoT All-Stars

IT is ready for IoT growth in today's environment

The most sophisticated "users" of IoT, All-Stars seek to make the most of IoT to influence the customer experience, further their competitive differentiation, and decrease time to market for new products and services. IoT All-Stars use IoT devices as change agents to take prescriptive or preemptive action – which in turn positively influences business outcomes or customer experience. IoT All-Stars are very strong users of related capabilities such as real-time data processing, causality and correlation analysis, and machine learning. All-Stars extensively reuse IT infrastructure and adopt next-generation development and delivery frameworks. All-Stars strongly focus on governance and compliance with mature and comprehensive data governance measures in place. To enable IoT, All-Stars use the broadest set of technologies (such as containers, automation, orchestration, and self-provisioning tools) in place for their IoT IT infrastructure. They have the best business KPIs of the four categories.

IoT Pros

IT is significantly ready for IoT growth in today's environment

In most ways, IoT Pros are like All-Stars who still have some work ahead of them. For IoT, they place emphasis on customer experience, competitive differentiation, and time-to-market. They are still sophisticated users of IoT. However, when it comes to their IT infrastructure, they fall behind All-Stars in makeup and usage. More than half employ IoT devices as change agents that take prescriptive action on their behalf, frequently using related capabilities such as real-time data processing, causality and correlation analysis, and machine learning. They have some IT infrastructure reuse and next-generation development and delivery frameworks. They place some focus on governance and compliance with some data governance measures in place. Pros enjoy better-than-average business KPIs.

IoT Rookies

IT is minimally ready for IoT growth in today's environment

IoT Rookies are more interested in minimizing cost and business risk than in how their investment in IoT IT infrastructure can improve their business. They take a narrower approach to IoT IT infrastructure compared with Pros. Like Pros, more than half of Rookies use their devices to take prescriptive action, but the usage of IoT endpoints is predominantly data-centric. They have little reuse of IT infrastructure and limited adoption of next-generation development and delivery frameworks. Their focus on data governance is less than ideal, with relatively weak regulatory and compliance measures in place. They have lower-than-average business KPIs.

IoT Amateurs

IT is unready for IoT growth in today's environment

IoT Amateurs take a very narrow view of IoT, seeing it as a risky strategy, and are most interested in minimizing cost and business risk. They have limited investment in IoT-related technologies and frequently their IT infrastructure is the least ready for IoT relative to the three other groups. They employ a much smaller number of technology components. Most of their IoT deployments are as sources of data capture for incrementally improving business decisions, and therefore they're limited in prescriptive action through IoT devices. Amateurs mostly do not reuse IT infrastructure nor employ next-generation development and delivery frameworks. Their focus on data governance is weak to nonexistent, and they have very few regulatory and compliance measures in place. Amateurs have the worst business KPIs of the four categories.



TABLE 1

IoT IT Infrastructure Readiness Category Profiles

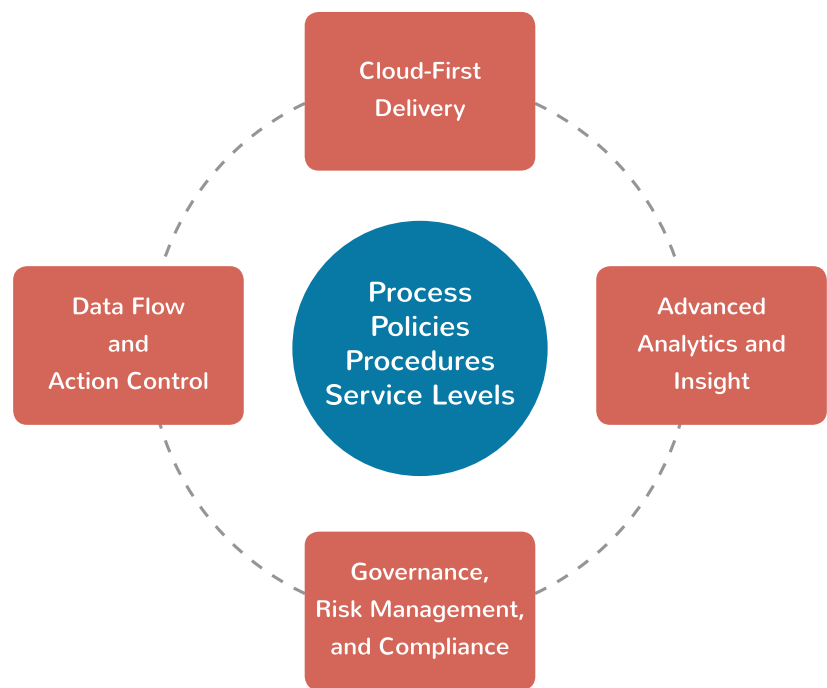
	IoT Amateurs	IoT Rookies	IoT Pros	IoT All-Stars
% of sample	16%	33%	35%	16%
Business drivers	Likely to emphasize minimizing cost and business risk	Likely to emphasize minimizing cost and business risk	Likely to emphasize customer experience, competitive differentiation, and time-to-market	Very strongly emphasize customer experience, competitive differentiation, and time-to-market
Processes	Highly unlikely to use IoT to take action	Unlikely to use IoT to take action	Highly likely to use IoT to take action	Almost universally use IoT to take action
	Highly unlikely to use data in real time, causality and correlation analysis, and machine learning	Unlikely to use data in real time, causality and correlation analysis, and machine learning	Frequently use data in real time, causality and correlation analysis, and machine learning	Very strongly use data in real time, causality and correlation analysis, and machine learning
Technology adoption	Highly unlikely to reuse existing IT infrastructure or use next-generation development and delivery frameworks	Unlikely to reuse IT infrastructure or use next-generation development and delivery frameworks	Likely to reuse IT infrastructure and use next-generation development and delivery frameworks	Highly likely to reuse IT infrastructure and use next-generation development and delivery frameworks
	Not likely to use a cloud-first delivery model	Likely to use a cloud-first delivery model	Likely to use a cloud-first delivery model	Highly likely to use a cloud-first delivery model
	Likely to employ a small number and variety of technology components in IoT infrastructure	Likely to employ an average number and variety of technology components in IoT infrastructure	Likely to employ an above-average number and variety of technology components in IoT infrastructure	Likely to employ a significantly greater number and variety of technology components in IoT infrastructure
Governance, Risk Management, and Compliance (GRC)	Likely to have very little focus on compliance and governance	Likely to have little focus on compliance and governance	Likely to have some focus on compliance and governance	Likely to have strong focus on compliance and governance
	Unlikely to have any IoT IT GRC measures in place	Likely to have weak IoT IT GRC measures in place	Likely to have some robust IoT IT GRC measures in place	Highly likely to have comprehensive IoT IT GRC measures in place

IDC IoT 2020 IT Infrastructure Readiness Indicators

IDC has developed a framework to assess and measure IoT IT infrastructure readiness (regardless of whether this infrastructure belongs to corporate IT, line-of-business IT, or Operations Technology). As Figure 1 illustrates, the IDC IoT 2020 Readiness Indicator focuses on four key “spokes” or areas bound together by corporate-wide processes, policies, procedures, and service levels. They are (1) Cloud-first Delivery Model, (2) Data Flow and Action Control, (3) Data Governance, Risk Management, and Compliance (GRC), and (4) Advanced Analytics and Insight. In this paper, we examine each of these areas to describe the differences between firms at various stages of IoT IT readiness.

FIGURE 1

IDC IoT 2020 IT Infrastructure Readiness Indicator



1 Cloud-first Delivery Model

The first indicator of IoT IT infrastructure readiness is the use of cloud-first development and deployment models and the ability to utilize dispersed assets and services. These include on- or off-premises cloud infrastructure and (to the extent they are allowed by industry regulations) public cloud services.

Firms must adopt an approach of delivering IT services and applications built on cloud-first development and deployment models to scale and flexibly respond to growth and market changes. Cloud-first need not imply an “all-in” approach into public cloud, which may or may not be an option for the firm. Rather, enterprises must have a vision that includes the ability to manage dispersed assets and services with agility, flexibility, and scalability that can be delivered in an OpEx-centric, metered fashion.

All-Stars and Pros have a greater propensity to use multiple types of cloud platforms for their IoT implementations and are more likely to use public cloud in IaaS implementations. In fact, more than 80% of IoT All-Stars use public cloud IaaS as part of their IoT infrastructure, as opposed to a mere 33% of IoT Amateurs. Presumably, these public cloud implementations are for collation of data along with causality and correlation analytics. More than half of IoT All-Stars use both public and private cloud for IoT, as opposed to 2% of Amateurs.

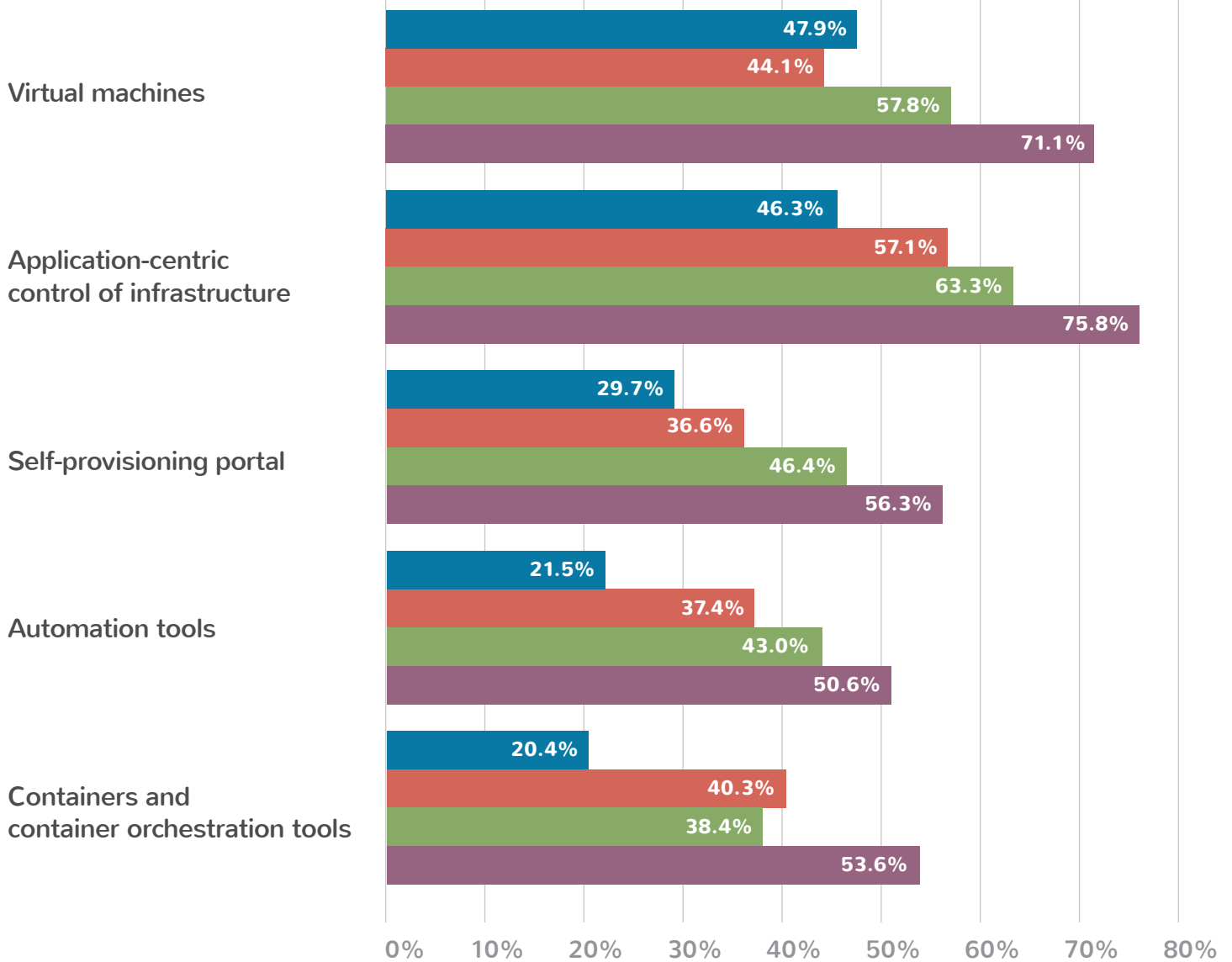
Note that using public cloud services (infrastructure, platform, or software as a service) is in and of itself not a direct indicator of IoT readiness because some markets and industries expressly forbid the use of public cloud. IDC is noting the use of public cloud as a supporting finding from the research and not its use by firms as a stand-alone factor in determining IoT readiness.

Firms are finding that they can reuse advanced infrastructure investments across multiple initiatives such as data analytics and cognitive applications. IoT All-Stars most commonly employ a combination of existing and new infrastructure for IoT, leveraging earlier investments in high-functioning infrastructure when appropriate and investing in new infrastructure when necessary. Contrast that to IoT Amateurs and Rookies, who are unlikely to be able to reuse existing infrastructure for IoT and therefore nearly half the time find themselves investing in brand new infrastructure.

Figure 2 illustrates that such firms employ more advanced technologies, are more open to making technology investments, and employ IoT across more platforms. IoT Pros and especially All-Stars more aggressively use technologies to get the full value out of their IoT infrastructure. This behavior makes good sense given the propensity of such firms to attribute business success to their IoT initiatives. These firms are doubling down on the strategy that already has yielded positive business results.

FIGURE 2

Components of Cloud-first Delivery Model



IoT Amateurs

IoT Rookies

IoT Pros

IoT All-Stars

IDC HPE IoT 2020 IT Infrastructure Readiness Indicator Survey, IDC, February 2017

Source: IDC, 2017

2 Data Flow and Action Control (Data vs. Action-centric IoT)

IoT requires use of a distributed data flow and control paradigms for compute and storage infrastructure, a strategy allowing the IoT infrastructure to span from massive datacenters at the core to micro-datacenters and intelligent devices in critical edge locations. This infrastructure is tied together (or controlled) by networks that may often lack reliable or economical connectivity, depending on the location and nature of the endpoints.

IoT All-Stars and Pros use distributed and advanced data flow and control for IoT IT infrastructure depending on the type of IoT devices in place. It gives them flexibility and elasticity in their infrastructure, enabling them to scale up or down as demands change.

IoT devices can take two potential roles in a deployment:

Data Sources (Data-centric IoT). IoT devices are first and foremost sources of data. Sensors can generate data related to their physical parameters, and many IoT devices can also generate contextual information that may be related to their operational conditions, location, or other physical parameters. Examples of IoT devices that act as sensors include video cameras, temperature gauges, vibration sensors, and connected cars. In terms of their role in the IoT infrastructure, these devices only send back information that the network can use.

Change Agents (Action-centric IoT). Advanced IoT devices may take prescriptive action based on the direct or contextual data they have generated. It is possible for a device to be both a sensor and a change agent. Examples of IoT devices that are active agents include smart building controls such as lighting or thermostats and machine controls on factory floors. These devices receive real-time instructions from the IoT network and adjust their behavior accordingly. A self-driving car is an example of a complex system of sensors and change agents that reports to the infrastructure its status and position and simultaneously receives back traffic data for use in determining its own best path of travel.

As Figure 3 illustrates, more than 70% of IoT Amateurs use predominantly data-centric IoT. These companies gather data from devices, but those devices don't play a significant role in improving business processes in real time. This usage hierarchy may reflect that gathering data, and more

importantly figuring out how to collect the right kind of data, is a prerequisite to taking any kind of action. Contrast that to All-Stars, of whom more than 95% employ action-oriented IoT. These firms are using their IoT infrastructure to enhance and improve business processes as a matter of course.

Many IoT IT All-Stars and Pros have a healthy mix of data gathering and action in their IoT infrastructure. That reflects how insight from data gathering is one of the very important benefits of IoT. In fact, a clear majority of All-Stars use their IoT IT infrastructure for both gathering data and taking prescriptive action. A good way to think about this phenomenon is that companies need the data from their IoT devices or they won't know what action to take. So, high-functioning firms do both.

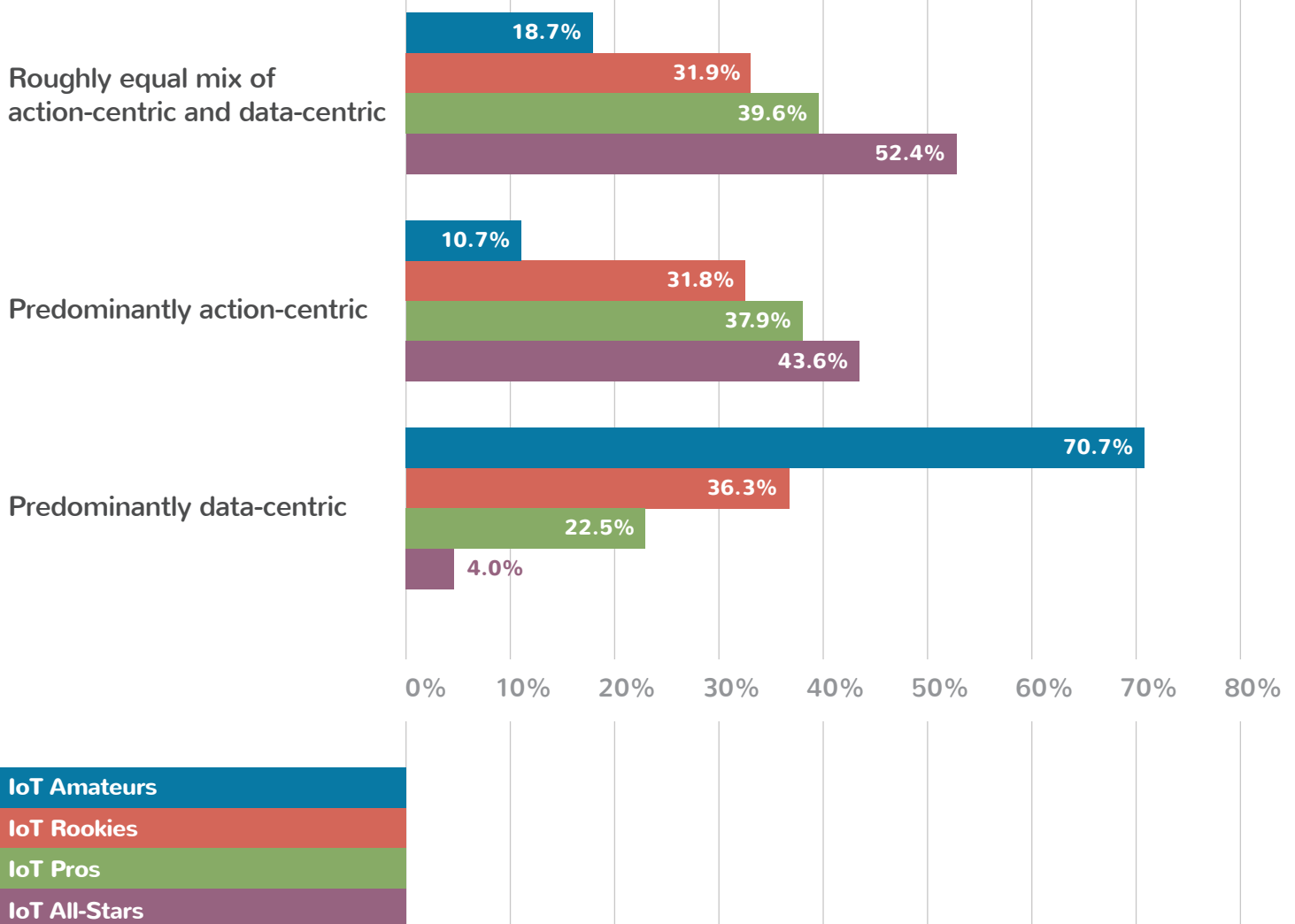
When asked about plans for geo-dispersed connectivity, 80% of All-Stars expressed their plans to increase the number of devices they use to capture data. Among IoT IT Amateurs, this number was 36%. While their environments are highly instrumented, All-Stars are not complete in their IoT vision and want to increase the visibility and automation of their systems.

All-Stars and Pros are also ready to expand the ability of their IT infrastructure to take prescriptive action. 68% of All-Stars state their intention to increase the amount of outbound command and control they exert over their devices, as opposed to 25% of Amateurs. Action-centric IoT necessitates that firms use data in more sophisticated ways. Real-time processing is a necessary requirement for action-centric IoT, and indeed higher-readiness firms are much stronger users of real-time data (at 54% for All-Stars as opposed to 15% for Amateurs).

FIGURE 3

Data Flow and Action Control

Q4. Which of the following best characterizes your organization's approach to IoT?



IDC HPE IoT 2020 IT Infrastructure Readiness Indicator Survey, IDC, February 2017

Source: IDC, 2017

3 Governance, Risk Management, and Compliance (GRC)

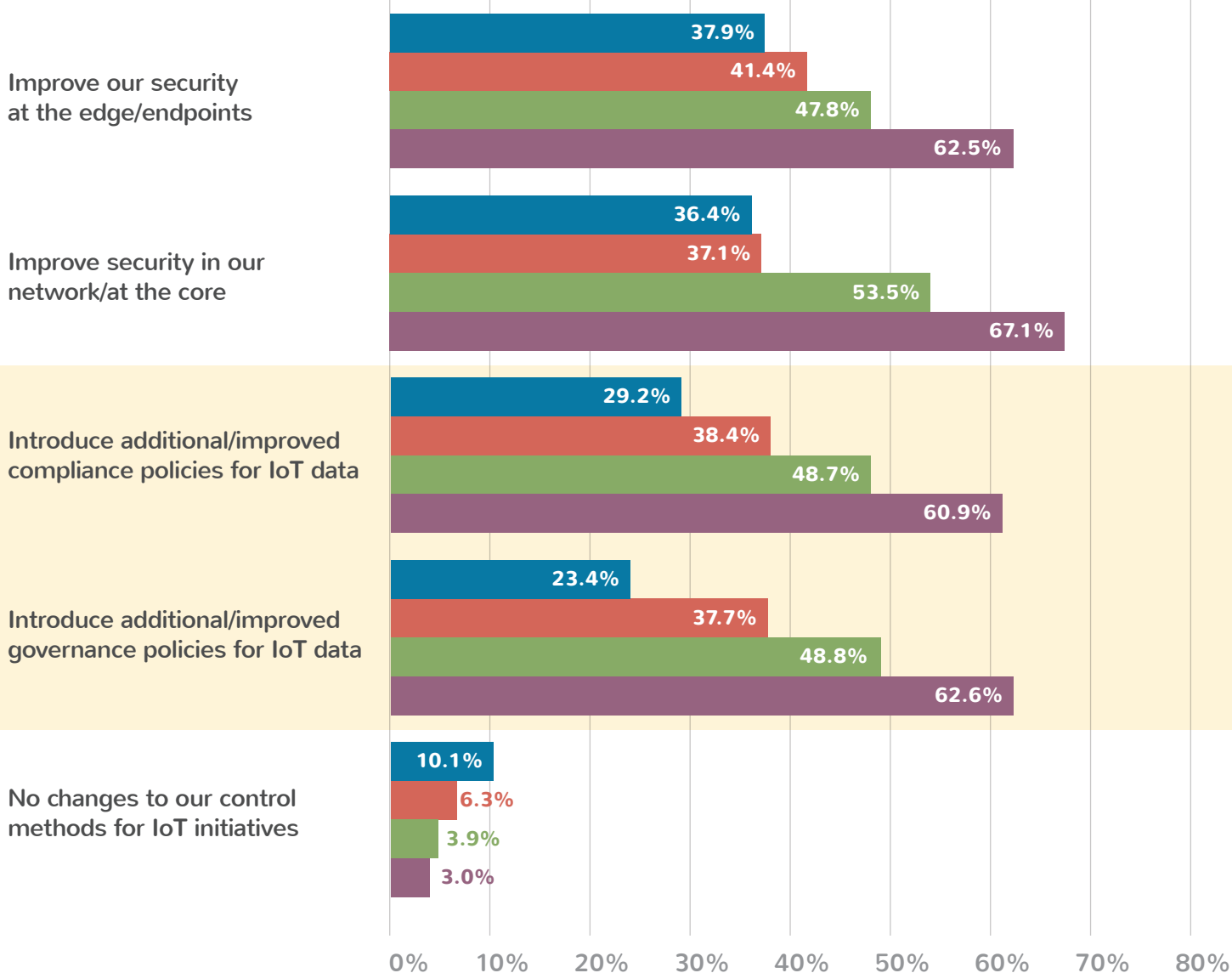
Data-related governance, risk management, and compliance is another area in which high IoT IT readiness firms stand out from others.

IoT All-Stars and Pros pay more attention to how and where they use data. They more actively seek processes for data governance, centralized compliance controls, and risk management than Rookies and Amateurs. They are prepared to make their environments compliant from core to edge and build dynamic risk management frameworks that can identify and adjust to changing threats. Pros and All-Stars are more likely to pursue a centralized data GRC strategy for their IoT IT infrastructure with a single group controlling the data and performing analysis against it. When it comes to planning for the expansion of data GRC, most IoT All-Stars intend to improve edge and endpoint compliance standards in addition to that of the network and core IT infrastructure. As Figure 4 illustrates, All-Stars and Pros examine opportunities for data compliance and governance policies for IoT data together.



FIGURE 4

Planned Data Governance Improvements



IoT Amateurs

IoT Rookies

IoT Pros

IoT All-Stars

IDC HPE IoT 2020 IT Infrastructure Readiness Indicator Survey, IDC, February 2017

Source: IDC, 2017

4 Advanced Analytics and Insight

Maximizing the business value of IoT requires organizations to analyze and gain insight from large data sets and have the future vision to reduce the complexity while accelerating prescriptive action from analyses. These efforts must be consistent and compatible with edge analytics.

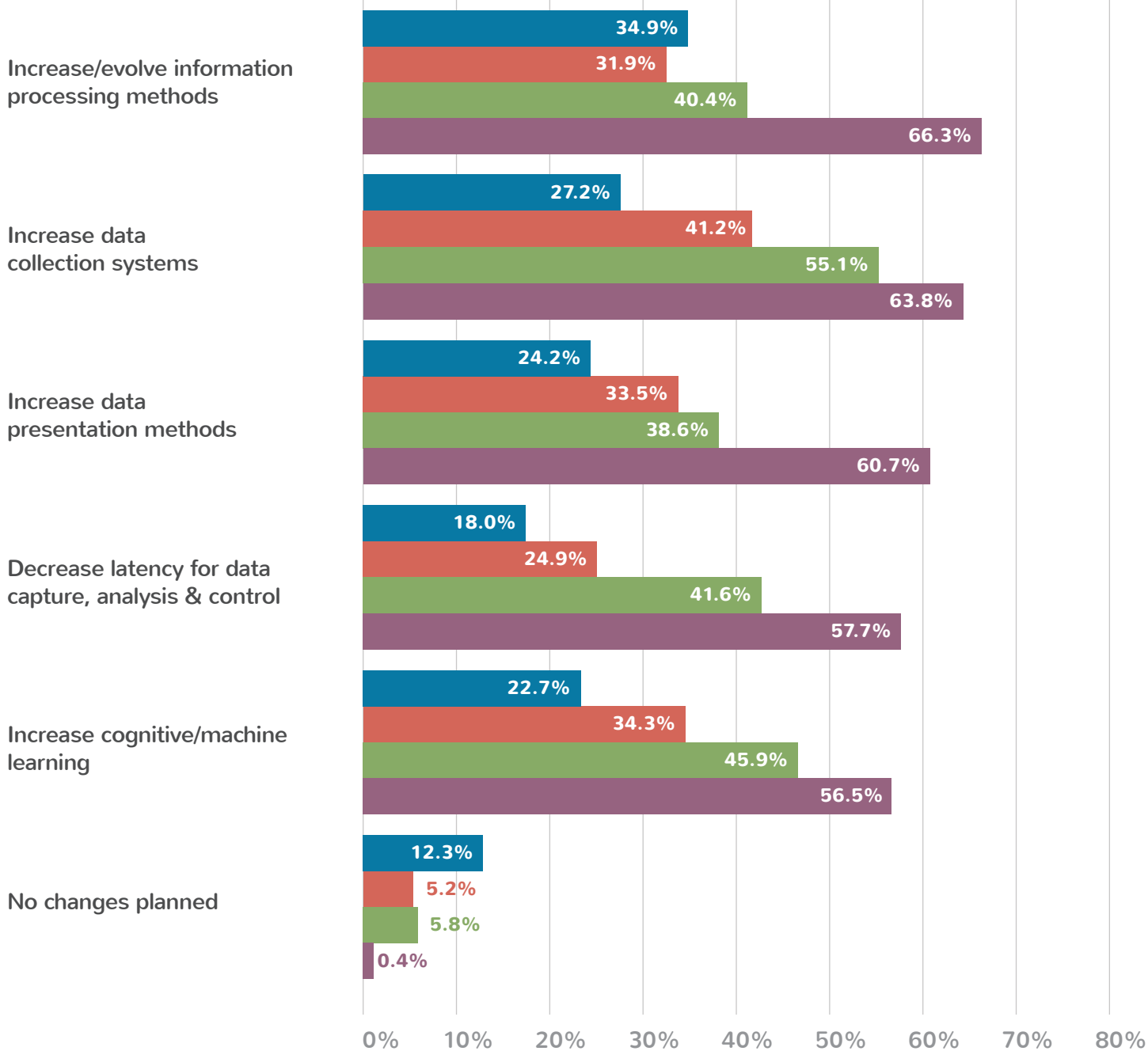
IoT IT All-Stars and Pros also collect more data sets and types, incorporate more kinds of endpoints, and aggregate data from more platforms, enabling them to “answer more questions.” Figure 5 illustrates IoT All-Stars’ bigger plans for evolving their analytics and control management for their IoT infrastructure, and more than 60% of IoT All-Stars plan to enhance their next-generation development and delivery frameworks for their IoT infrastructure, as opposed to 21% of Amateurs.

Finally, advanced analytics mechanisms (like cognitive and machine learning in areas such as pattern recognition, behavioral analysis, and predictive maintenance) and IoT infrastructure readiness are symbiotic. Firms should have a vision to use cognitive and machine learning to automate decision making and prescriptive action. Here we see perhaps the starkest difference between IoT IT All-Stars and less ready companies. Cognitive and machine learning systems often use data to provide advanced inference and training capabilities for products and services. Examples include using video analytics to monitor and route traffic within warehouses, facial recognition services, and anomaly and fraud detection services. 84% of All-Stars use causality and correlation analysis as opposed to 13% of Amateurs. More than half of All-Stars currently have cognitive or machine learning algorithms in production, while only 1% of Amateurs do. This difference in use of cognitive systems ties to the differences in using IoT devices for prescriptive action. Real-time action in a complex network of devices requires the use of advanced computing capabilities, so firms taking on the effort of using devices for prescriptive action are strongly aided by cognitive systems.



FIGURE 5

Advanced Analytics and Insight



IoT Amateurs

IoT Rookies

IoT Pros

IoT All-Stars

IDC HPE IoT 2020 IT Infrastructure Readiness
Indicator Survey, IDC, February 2017

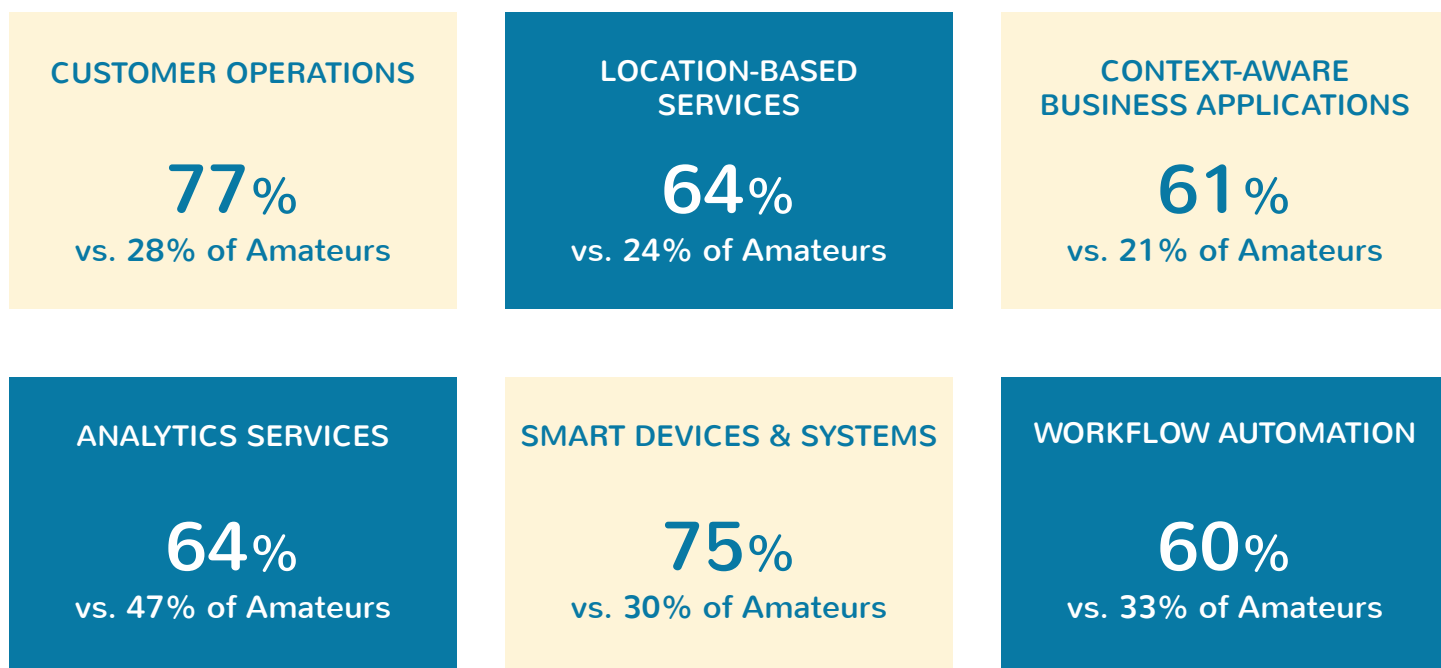
Source: IDC, 2017

IT Infrastructure Readiness and **Business Outcomes**

High IoT IT readiness firms are driven by business outcomes, focusing on customer success and the factors that drive that success over cost when utilizing IoT information (Figure 6).

FIGURE 6

IoT **Readiness** and **Business Outcomes** for IoT **All-Stars**



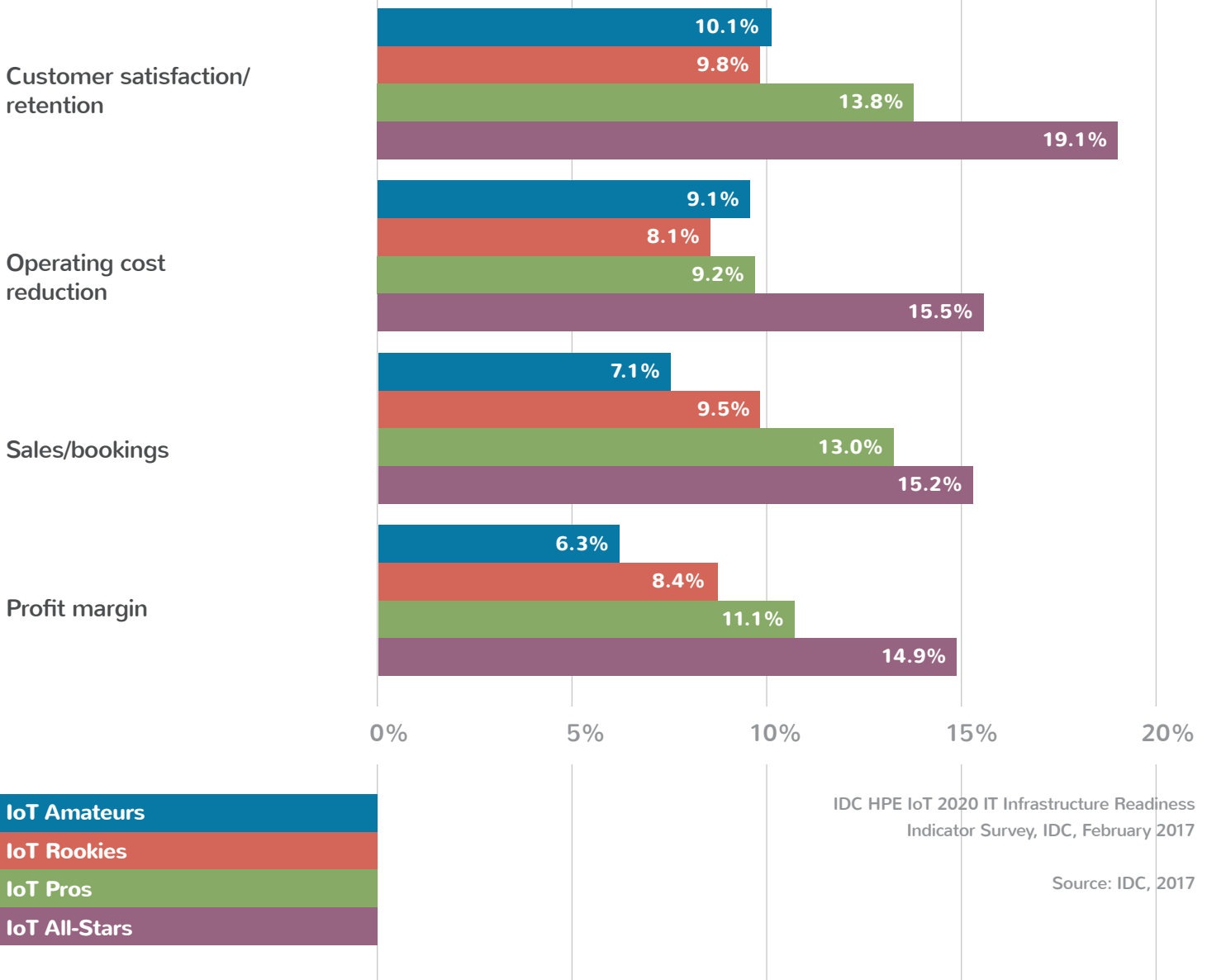
IoT IT Infrastructure Readiness **Drives Positive Business Results**

IoT IT infrastructure readiness directly correlates to positive business results and performance, which is to say it has positive and measurable return on investment. (Note: To qualify, respondents needed to be part of firms with an IoT strategy in place or imminently in place.) Amongst firms in the survey, high IoT IT readiness firms enjoy much

better performance than those less ready. 87% of IoT All-Stars report that IoT has driven significant or major business improvement, and more than half of IoT Pros report significant or major improvement. In short, an IoT-ready IT infrastructure directly enables firms to realize their strategic IoT-centric business objectives.

FIGURE 7

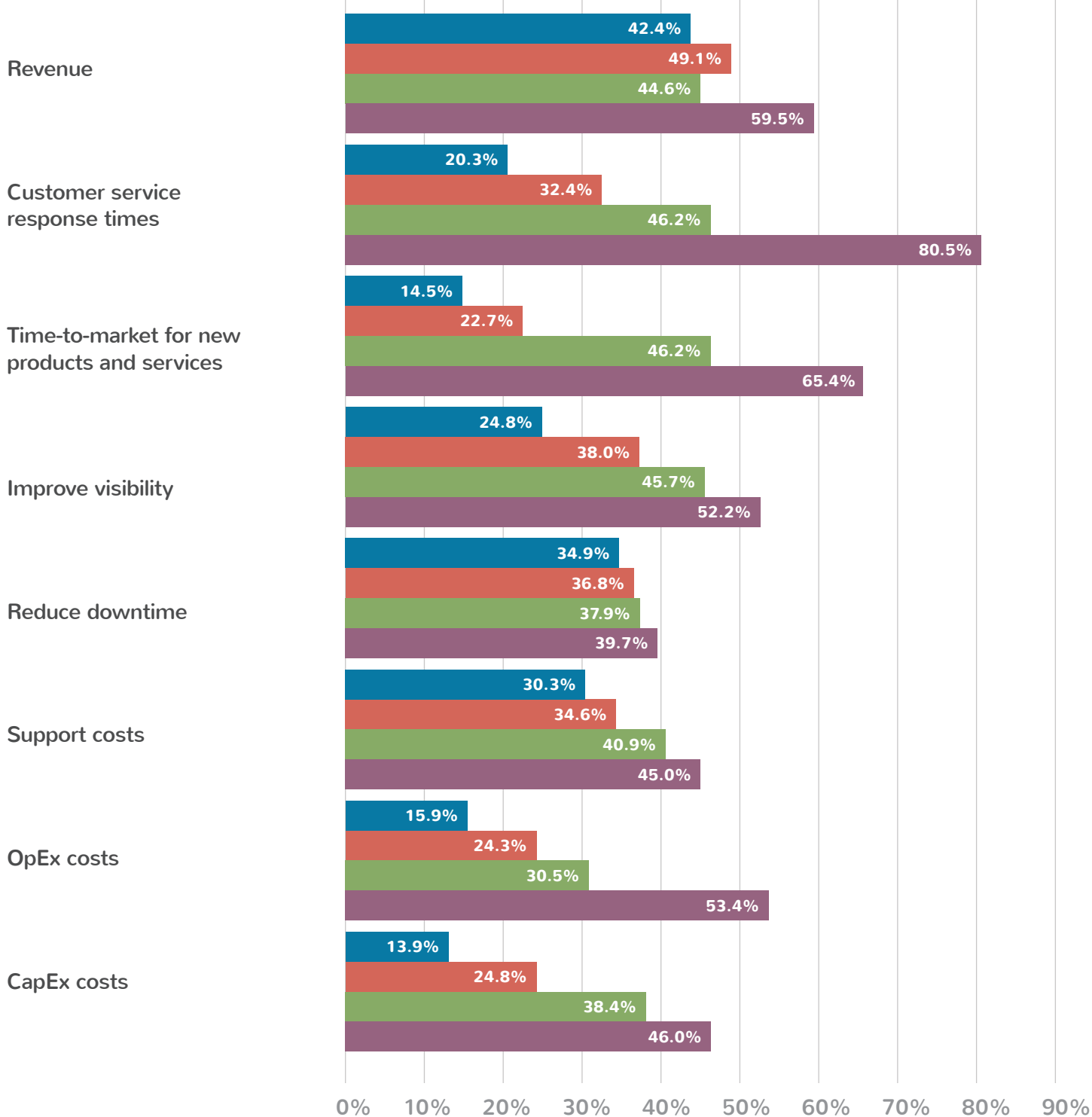
Improvement in **Key Performance Indicators** by IoT IT Readiness



Figures 7 and 8 illustrate the connection between IoT IT Infrastructure readiness and business outcomes. A compelling differentiator of high IoT IT readiness firms is their level of interest in advanced business outcomes resulting from investments in IoT. Such firms, especially IoT All-Stars, take keen interest in more sophisticated and nuanced business drivers like customer experience, new revenue streams, and competitive differentiation. Rookies and Amateurs, on the other hand, focus more on revenue, cost reduction, customer service response times, and time-to-market for new products and services. While this second set of factors is crucial, it can be considered table stakes for all IoT initiatives. In most instances, improving the first set of metrics will ultimately translate to top-line revenue results.

FIGURE 8

Metrics or Success Criteria Used to Measure **Return on Investment in IoT**



IoT Amateurs

IoT Rookies

IoT Pros

IoT All-Stars

IDC HPE IoT 2020 IT Infrastructure Readiness Indicator Survey, IDC, February 2017

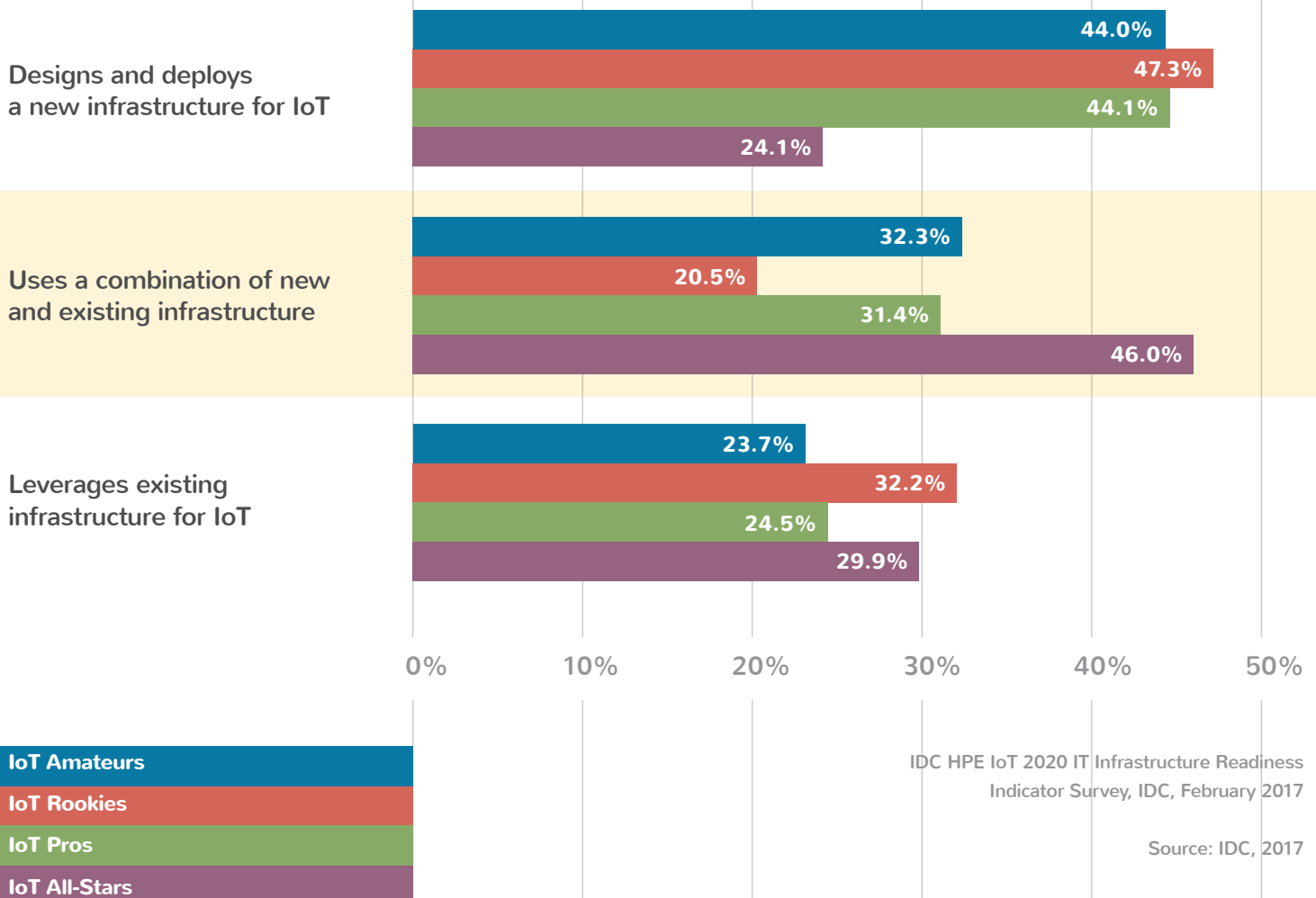
Source: IDC, 2017

Maximizing Investment in IT Infrastructure

Figure 9 illustrates that IoT All-Stars tend to make the most of existing IT infrastructure investments for IoT initiatives. They complement existing infrastructure with new components where necessary. Doing so gives them the flexibility, scalability, and agility they need to accommodate changing applications, data analytics frameworks, and governance standards. IoT is one beneficiary of this approach.

FIGURE 9

Maximizing Investment in Existing IT Infrastructure



Firms seeking to improve their IoT IT infrastructure readiness should focus on three key areas

Commit to the "Big Picture"

Choose an IoT strategy that affects your core business in a disruptive fashion rather than one that provides benefits that are more peripheral or incremental in nature.

Focus on business outcomes

The right IoT IT strategy can directly improve key business metrics such as customer retention, average deal size, and industry ranking. IoT initiatives can not only increase new revenue streams, but also generate a more diverse revenue mix and promote competitive differentiation. IoT initiatives that directly affect customers or improve core differentiators may require businesses to transform, and when executed properly, this transformation can be highly impactful. High IoT readiness firms depend heavily on data-centric insights to improve customer experience and therefore business outcomes. They look at opportunities in their IoT infrastructure to gain timely insights, which warrant investing in the right infrastructure, data, and application portfolio.

Invest early and consistently

Once your firm has a clear understanding of its IoT strategy, begin right away and commit to adequate funding for the initiative. Earlier execution yields earlier benefits, accelerating transformation within your firm, but it must be aligned to the IoT and organizational goals. Investment is especially time-critical if IoT can be a meaningful differentiator over the competition. Firms must ensure that IoT investments provide the functionality, flexibility, and scalability, or IT could be the weak link in your overall IoT chain. Ability to scale IoT projects from proofs of concept is a great litmus test for whether your investment in existing IT infrastructure is adequate. Firms should identify ways in which a production environment can scale to two or three times the scope of a full-scale proof of concept without difficulty.



Data, Applications, and Infrastructure

Getting a good return on your IoT investment requires an equitable investment in a modern IT infrastructure and application portfolio. Employ modular and flexible IT infrastructure design built of scalable, agile components and technologies. Your infrastructure must operate as a service-ready entity with resources you can compose on demand. When designed as a part of a big, datacenter-wide modernization initiative, this infrastructure can also support other advanced computing initiatives such as cognitive computing, Big Data and analytics (including real-time/streaming analytics), technical/supercomputing, next-generation application development and delivery, and edge computing (which could be part of your IoT initiative as well).

Invest adequately

Ensure that investments in this infrastructure are adequate in scale (capacity and performance) and operational efficiency (people, process, and technology) to meet your coming needs, not just for IoT but also for other digital initiatives. Underinvestment in the early days can lead to scale and operational limitations that later force unplanned spending, increasing total investment cost over the project's life cycle. To move toward higher IoT readiness, firms should align their IoT IT infrastructure investments to other business initiatives and vice versa. Consult IDC's four-point IoT IT Infrastructure Readiness Indicator framework to ensure you are building out a future-ready IoT IT infrastructure.

Avoid the "either/or" trap

When making infrastructure selections, firms must be cautious of "either/or" traps, decisions that lead to compromises in one area or limit others. There are many paths to success, and specific circumstances may direct firms toward specific options. As an example, one crucial infrastructure strategy requires selecting the right premises (on-premises and off-premises) and deployment model, to the extent permissible by industry regulations (private cloud, industry clouds, public infrastructure services, or even traditional non-cloud infrastructure). IDC finds that moving toward a higher state of readiness often requires firms to embrace a "hybrid IT" strategy, which (to the extent allowed by industry regulations) could involve investing in infrastructure both on- and off-premises and in private and public clouds. All these options have pluses and minuses, and there is no such thing as a "one size fits all" approach. Some IoT applications cannot utilize public cloud due to data governance requirements such as business covenants, security constraints, or governmental regulations, and for them private cloud is the best option. Wherever it makes economic, business, and regulatory sense, firms need to examine public cloud options. IT architects need to partner with LOB application owners and developers to develop a long-term strategy rather than being driven purely by short-term revenue savings.

Think about edge intelligence

IDC believes that 43% of all IoT-generated data will be preprocessed at the edge by 2020. Firms need to consider investing in "edge intelligence" to make real-time analytics-based decisions. These include inference and training activities as well as scrubbing data before sending it to the cloud (prevent unnecessary costs by sending and storing only the required data). More importantly, edge computing options like these minimize the possibility of inundating the core datacenter infrastructure and streamline data flow and control across the entire IoT IT infrastructure.

Carefully consider where you start

When considering what data to collect and how to use it, start with a broad-minded approach. Look holistically at your business and how “connected devices” fit with the organization’s objectives. Doing so will yield higher-quality insights than simply monitoring a set of obvious straightforward metrics that may not contain the information needed to transform. Be sure to focus on a combination of insights and the actions you can take, and consciously plan future expansion. For example, it might make sense to start with a project for which data is readily accessible and minimal organizational change is required. Once this project is operational, the business can expand by adding sensors or actuators, applying them to currently unmeasured processes, or using previously internal data to augment customer-facing applications.

Customize your applications

Firms with high IoT readiness are heavy users of custom (and often next-generation) software applications for their IoT infrastructure. That’s because the business outcomes and hence the technical requirements for IoT are often highly specific, and off-the-shelf applications will not always do a proper job. Furthermore, firms looking to provide a differentiated customer experience may not want to use an off-the-shelf application that provides limited ability to differentiate. Firms need either to obtain the skills and tools to create their own custom applications or to identify a partner who can serve that role for them.

Expect to scale

Finally, firms must factor in unexpected growth in the amount of data they may have to collect to improve the richness of the IoT experience. The IoT infrastructure will no doubt collect, process, and store exponentially more data as their reliance on IoT increases and becomes more sophisticated and comprehensive.



Security and IoT Readiness

This study focuses on IT infrastructure readiness by examining key infrastructure attributes that apply to IoT environments. Attributes such as deployment model; data flow and action control; governance, risk management, and compliance; and advanced analytics and insight are important. However, firms often consider security in particular to be foundational to the entire enterprise and not an isolated infrastructure deployment. IoT is no exception. Security considerations continue to be of utmost importance for IoT initiatives. In fact, a recent study by HPE subsidiary Aruba Networks found that 84% of customers with IoT deployments have experienced a breach in their IoT environments. IoT introduces two significant new factors into security considerations: Plan for systems to minimize, and have a response plan.

IoT implementations effectively increase the attack surface for any organization

Attack surfaces increase because IoT devices are not replacing existing technologies but rather adding new or formerly unconnected objects, processes, or machines. Transforming business processes with IoT devices will likely create exponential growth of device data, which will then require monitoring, security, and curation like the traditional IT devices already in place.

Many IoT devices require non-traditional management

Some IoT devices require new security approaches. Some devices contain traditional operating systems and may be secured by professionals familiar with basic IT security techniques. However, many connected technologies often contain unique operating systems without the benefit of easy-to-access management capabilities. Sensor technologies, for instance, are designed for singular purposes, with heavyweight operational mechanisms removed in the name of efficiency.

These factors leave little opportunity to execute on the scan-and-remediate strategy to which IT security professionals have become accustomed.

Considering the difficulty in retrofitting existing security technologies on top of newly implemented IoT, firms have begun to investigate other techniques. User and entity behavior analytics (an analytics process that determines abnormal user or device behavior) have become a popular mechanism to discover compromised devices, bringing with them a resurgence in network access control (NAC) mechanisms to automate removal of misbehaving devices.

Whatever the specific technology, the key takeaway is that IoT devices will likely be unprotected by in-place solutions. Firms need to ensure they understand the impact an IoT implementation might have on their security posture before plunging headlong into a new solution. They need to carefully consider proposed technological improvements and the possibility of overwhelming staff with the scale and nuisance of deployments. Pay attention to architectural changes that may occur, like control platforms or data stores moving from on-premises locations to cloud platforms.

The following questions can guide your security assessment processes:

- How many IoT devices will be deployed, and what is the net increase in security management responsibility?
- Do devices easily fit within existing security parameters or management techniques?
- Is the source of the devices trustworthy?
- Will devices or new business processes materially alter data storage locations or data transfer patterns? Is there enough ephemeral and persistent network and storage capacity in the existing infrastructure to store data generated by these devices?
- Are device-to-device, device-to-edge, and edge-to-core communications encrypted?
- Is data stored or encrypted on the device itself?
On the wire?



CONCLUSION

IDC's IoT 2020 IT Infrastructure Readiness Indicator is a framework and road map for creating a future-ready IoT approach. This framework defines four aspects of how mature organizations excel in their IoT strategies and improve their IoT IT infrastructure readiness.

Cloud-first delivery model

Moving toward high IoT readiness means utilizing a cloud-first delivery model for infrastructure, whether public, private, or hybrid cloud. Such a delivery model offers the agility, scalability, and flexibility to grow IoT projects in scope and geographic footprint. In the long run, this approach is both CapEx- and OpEx-friendly.

Data flow and action control

High IoT IT readiness requires employing more advanced data flow and action control mechanisms in IT infrastructure. Focus on identifying, routing, and analyzing the right data sets. Enable proactive action using core- and edge-based data analytics to enable real-time or near real-time inference and training. Processing data prior to sending it upstream or even employing autonomous decision making (particularly when connectivity or cost concerns are a factor) can streamline information workflow and speed insights.

Advanced analytics and insight

High IoT IT readiness firms utilize advanced analytics to gain actionable and timely insight into data. They take advantage of advanced technologies such as accelerated computing, machine learning, and cognitive systems to improve agility and the quality of insights. To move up the readiness spectrum, seek to hone these capabilities, advancing from simple data aggregation to actionable insight. Use deep intelligence not just at the core but also by pushing control out to edge computing devices.

Data governance, connectivity, and compliance

The more IoT-ready the firm, the more robust its governance, risk management, and compliance framework. High IoT readiness firms have learned how to incorporate IoT data, applications, and infrastructure into existing GRC frameworks, which themselves are updated to make sense in the era of connected devices.

Firms seeking to be best-in-class should ensure they consciously build out the right infrastructure to support their organizational strategies. They should move forward with technology investments early to ensure quick results. They should concentrate on IoT use cases that will directly contribute to a fundamental business mission, positively affect customer experience, or actively differentiate them from competitors. Firms should be prepared to create customized software applications to fit their specific business needs, and they should ensure that governance, compliance, and security are sufficient and appropriate to protect their infrastructure, data, applications, and users.

In closing, a crucial source of differentiation between firms with different levels of IoT readiness is their attitude toward IoT. High IoT readiness firms view IoT as a key enabler of mission-critical and long-term business initiatives. They continually seek to enhance the capabilities of their IoT IT infrastructure, complementing it with data and application capabilities where applicable. Increasing readiness requires a shift in attitude at the highest management levels of the organization. It requires firms to commit to a journey that can be both disruptive and transformative, one that will carry them deep into the future digital age.

Remember, these are still the early days of IoT. Readiness is a journey that won't end anytime soon, and all firms, even All-Stars, need to continue to disrupt and evolve as they invest in IoT.

Data-centric vs. action-centric IoT

In developing their IoT capabilities, most firms start with **data-centric IoT**. This strategy can help improve existing business processes and to some extent sets the stage for a long-term business transformation. Data-centric IoT is about harvesting data from existing sources and adding in news sources to provide new answers. The primary focus of this IoT model is to collect or stream data from end-points to the core, a centralized data hub that serves as the location for the analytics necessary to identify tactical or opportunistic issues. The amount of data flowing back to devices is relatively small, and there is little device-to-device communication or interaction.

As firms evolve in their IoT capabilities they tend to shift away from a pure data-centric approach to increasing levels of **action-centric IoT**. This strategy builds on the data-centric approach by introducing bi-directional interaction. In addition to collecting and analyzing data from endpoints to the core, firms can now take preemptive action to prevent a certain condition or take corrective action to remedy it. These endpoints themselves must be part of a system that is highly interactive and connected by a constant, bi-directional communications network. Action-centric IoT is all about real-time analytics, and it completely changes the way firms can harness and analyze data.

Data-centric IoT introduces the concept of core-to-edge-to-endpoint, where “edge” is an intermediary between endpoints and the core. It enables hub-and-spoke data collection and analysis to reduce network traffic and can enhance causality and correlation for various data sources. In action-centric IoT, the role of the edge significantly increases as the edge becomes an intermediate and often an autonomous control hub to speed decision making and minimize data transfer to the core.

In many industries, data-centric IoT is table stakes. It enables firms to dip their toes into IoT and figure out ways to gain competitive advantages by mining data from newly connected devices. Mostly this effort searches for pointers in tackling specific issues. These pointers can deliver significant incremental improvements to existing business

practices but do not disrupt a business completely. Over time as technology matures, business processes become IoT-friendly, and regulation catches up, firms can introduce action-centric IoT to the mix.

An action-centric IoT-based strategy, truly brings DX to the masses. It can completely transform a firm or an industry by introducing entirely new sources of competitive differentiation and can even change the lifestyles of workers and consumers alike. Action-centric IoT is best suited for new firms seeking to disrupt markets, but it also is embraceable by existing organizations that want to take a transformative approach to their own businesses. Firms well-entrenched in data-centric IoT that wish to go to the next-level can also make the shift to action-centric IoT. Such is the scale of this transformation that by 2018 IDC believes that one-third of leaders in each industry will be disrupted by competitors whose business models will be entirely built on connected experiences, and these experiences will be enabled by IoT systems.

A good example of this transformation can be found in the insurance industry. Today carriers are installing devices in vehicles to monitor driving habits, gauge risk factors, and adjust customers’ premiums based on their revealed risk profiles. Much of this information today is asynchronous. Slowly the industry, in collaboration with automobile manufacturers, is introducing enhancements such as the ability to provide real-time feedback to drivers on how they are driving and taking basic action such as alerting authorities when driving anomalies are detected. Eventually, firms may begin using in-car devices to communicate with each other to avoid on-road risks in real time or even to interact directly with vehicles to reduce the risk of accidents. All these developments have the potential to not only dramatically improve insurance cost curves but also to provide a greatly improved experience for the people in those vehicles.



Next Steps

We know your business is about creating simple, effective solutions for your customers. We make it our business to make sure you're IoT-ready. Reach out to your channel partner or HPE representative to get started today.

Prepare for Billions

The IoT 2020 IT Infrastructure Readiness Indicator

An IDC Thought Leadership
White Paper

Sponsored by:



Hewlett Packard
Enterprise



IDC Global Headquarters
5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit idc.com/about/wwoffices.jsp. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2017 IDC. Reproduction without written permission is completely forbidden.