IDC FutureScape

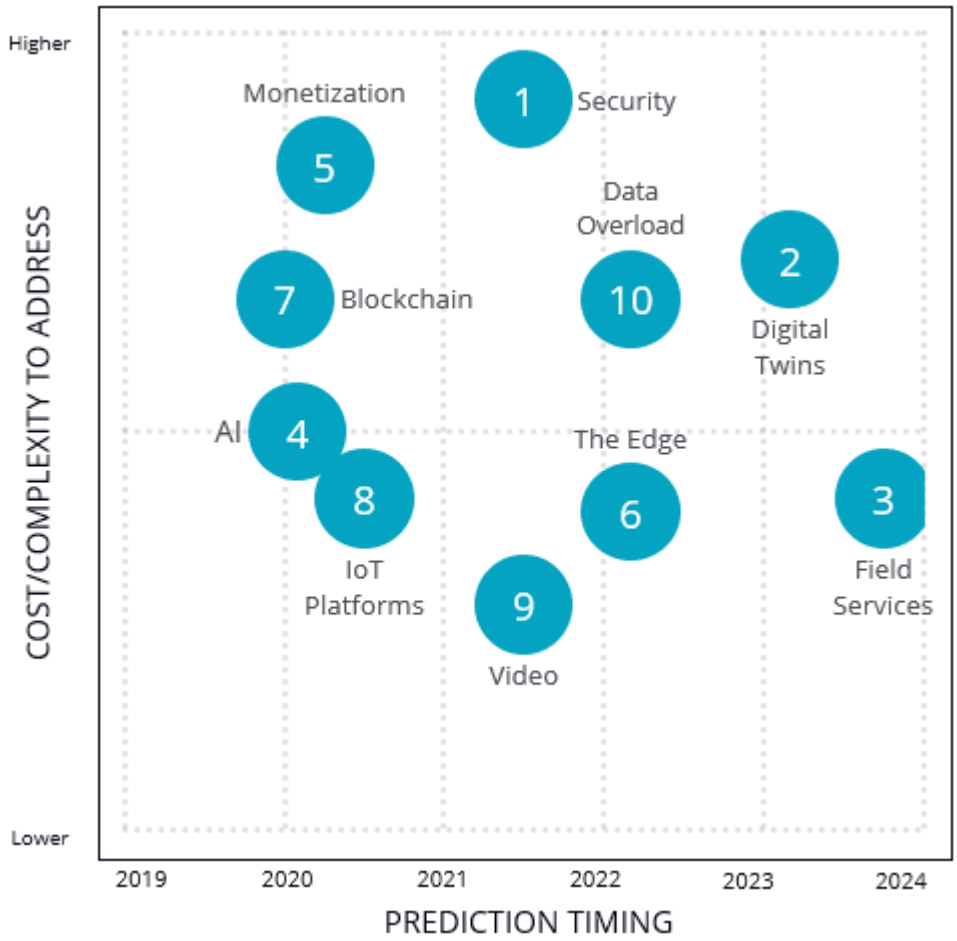
IDC FutureScape: Worldwide IoT 2019 Predictions

Carrie MacGillivray Stacy Crook Maureen Fleming Jeffrey Hojlo
Ashish Nadkarni Aly Pinder Hugh Ujhazy Robert Westervelt
Marta Muñoz Méndez-Villamil

IDC FUTURESCAPE FIGURE

FIGURE 1

IDC FutureScape: Worldwide IoT 2019 Top 10 Predictions



Note: Marker number refers only to the order the prediction appears in the document and does not indicate rank or importance, unless otherwise noted in the Executive Summary.

Source: IDC, 2018

October 2018, IDC #US44390618

EXECUTIVE SUMMARY

Internet of Things (IoT) remains one of the top digital transformation initiatives happening across organizations today. While much of the focus has been on digitally enabling the physical, we are seeing IoT move into its next chapter as the harmonization between human and machine begins to happen. IoT underpins the exchange of information from "things," people, and processes. Data becomes the common denominator and it enhances our senses and business processes by providing critical visual, audio, tactile, and environmental queues that allow us to adjust, adapt, and react to changing conditions in the world around us.

IDC's worldwide IoT team has collaboratively built our view on some of the key topics we expect to affect businesses over the next few years. This year's IoT predictions are:

- **Prediction 1:** Over 50% of G2000 companies will have modernized and IoT enabled their industrial control systems by 2021 without addressing cybersecurity or public safety concerns, prompting regulators to legislate.
- **Prediction 2:** By 2024, 50% of manufacturers will network related product and asset digital twins into digital twin ecosystems for a systems-level view of their business and 5% reduction in cost of quality.
- **Prediction 3:** Despite supply chain complexity hindering innovation, 50% of manufacturers will have implemented predictive field services across connected assets to improve delivery speed and customer value by 2024.
- **Prediction 4:** By 2020, the success rate of AI implementations in IoT will have reached 90%, with the major factor behind this success being collaboration between data scientist and engineering teams.
- **Prediction 5:** By 2020, over 30% of IoT initiatives worldwide will fail to demonstrate a clear ROI, with organizations lacking the necessary KPIs to monitor progress from the early stages of such projects.
- **Prediction 6:** With 40% of initial IoT data analysis occurring at the edge by 2022, organizations will invest more in gateways to aggregate and analyze edge data, especially in the context of IT, OT, and CT systems.
- **Prediction 7:** In 2019, blockchain's limitations in processing vast numbers of IoT transactions in real time will limit IoT integration into blockchain and thus IoT-related spend to 5% of overall blockchain spend.
- **Prediction 8:** By 2020, 70% of organizations will leverage commercial IoT platforms to develop and deploy IoT applications, and more than 50% will have multivendor IoT platform environments.
- **Prediction 9:** By 2021, 45% of video surveillance content will be used to provide context to data from IoT endpoints in public safety scenarios and in transportation hub and campus monitoring, among others.
- **Prediction 10:** By 2022, problems aggregating and rationalizing sensor data into actionable insight will have forced 20% of large manufacturers to insist on OEM data being reconciled in IoT data exchanges.

This IDC study provides details behind IDC's top 10 predictions for IoT for 2019 and beyond.

"The next chapter of IoT is just beginning as we see a shift from digitally enabling the physical to automating and augmenting the human experience with a connected world," says Carrie MacGillivray,

group vice president, IoT and Mobility. "Our IoT team continues to keep a pulse on the latest market developments to help inform enterprise decision makers as they look to use the audible, visual, tactile, environmental, and contextual inputs that IoT provides to digitally transform their business."

IDC FUTURESCAPE PREDICTIONS

This study provides IDC's top 10 predictions for the 2019 IT buyer when it comes to evaluating and investing in IoT solutions. The topics addressed cover some emerging technologies that intersect with IoT but also some of the existing solutions that are evolving based on market demand.

IDC covers IoT across several dimensions including hardware, software, services, and connectivity domains as well as through the industry lens where IoT is increasingly seeing vertically specialized solutions built. This document contains detailed inputs from IDC's global IoT team on major trends, with advice for IT buyers to consider in their IoT-related planning.

We advise decision makers to approach each prediction in three steps:

- **Assess its relevance.** Should I pay heed to this prediction? Does this prediction apply to my business? Can I reasonably enough ignore it? What do I risk if I ignore it? Strategy is, after all, as much about what you decide to do as what you decide not to do.
- **Assess its urgency.** Does it apply to me now or in the future? If it applies in the future, when do I have to get started to deliver enabling capabilities as needed?
- **Assess its resource requirements.** What resources do I need and at what costs? What would I have to forego or postpone to achieve the capability? What do I have to speed up to achieve it?

Table 1 provides the key elements behind the IDC FutureScape predictions.

TABLE 1

Key Elements of an IDC Prediction

Element	Description
Driver	Drivers include external factors that set conditions for each decision imperative. Drivers must directly influence the decision and typically fall into the following categories: political, economic, social, technological, environmental, legal, and business. Decision makers do not have control or influence over such factors.
Prediction	Predictions are written from the technology decision maker's perspective and describe either actions taken in response to a set of drivers to achieve a business or technology outcome or market condition or vendor actions or policies.
IT impact	IT impacts describe internal forces relevant to actions compelled by the imperative, IT actions in response to compelling internal forces, and the consequences of internal forces and actions taken.
Guidance	Guidance is specific, practical, and actionable advice provided within IDC's direct sphere of technology and industry expertise.

Source: IDC, 2018

Summary of External Drivers

Many external factors have a direct or an indirect impact on the future of the IoT landscape and on IDC's predictions for the future of IoT as a key innovation accelerator of digital transformation (DX). They come from business, social, economic, and technological realms. IDC has identified six drivers that represent significant forces affecting the evolution of IoT within the enterprise. Collectively, these drivers lead to the 10 predictions discussed in the sections that follow.

The drivers for IDC's 2019 IoT predictions are:

- **Cyber insecurity**: Theft, cyberattack, and negligence create a crisis of digital trust
- **Next chapter of DX:** Technology-driven transformation altering business and society
- **Platforms, platforms, platforms:** Industry competes for innovation at scale
- **The race to innovate**: Speed of change, delivery, and operations separates thrivers and survivors
- **Reimagining the material world:** Revolutionized processes expand technology reach
- **Sense, compute, actuate:** Turning data into value

More detail on the external drivers can be found in the External Drivers: Detail section at the end of the document.

Predictions: Impact on Technology Buyers

Prediction 1: Over 50% of G2000 Companies Will Have Modernized and IoT Enabled Their Industrial Control Systems by 2021 Without Addressing Cybersecurity or Public Safety Concerns, Prompting Regulators to Legislate

The deployment of modern components to manage industrial control environments has prompted organizations to embrace internet connectivity and cloud-delivered solutions, in the spirit of reducing costs and improving productivity in operational environments. But cloud adoption and increased connectivity in operational technology (OT) environments expand the attack surface and security researchers are pointing out some glaring weaknesses in both legacy and newly introduced devices that increase the potential for attacks driven by external threat actors. These environments can now be probed by financially motivated attackers serving up ransomware, nation-state threat actors intent on stealing intellectual secrets, and even corporate espionage and sabotage activity from nefarious competitors.

The news headlines validate some of this activity. Automobile manufacturers, distributors, and other businesses had been forced to shut down production lines as a result of ransomware outbreaks or the threat of such disruptive activity. In addition, security consultancies that create power management system honeypots that represent real-world environments to identify malicious threat actors and monitor and record their activities have documented utility company attack activity that appear to be part of intelligence gathering operations. This research followed a spate of high-profile attacks, including a sabotage operation in Ukraine against utilities and power generators disrupting them for more than 7 hours before power was brought online. There have also been many documented cases of the use of custom malware to maintain persistence and eavesdrop on U.S. energy companies.

An IDC survey of 400 companies using or evaluating "data services for hybrid cloud" had some key security findings from manufacturers, energy sector businesses, and other organizations that maintain industrial control system environments. Gaining real-time insights or the ability to analyze data in real

time was a top challenge, but nearly 60% of those surveyed cited challenges ensuring data quality, meeting corporate governance rules, and ensuring visibility and control over sensitive data. As accelerated investments in digital transformation cross the IT divide into operational technology environments, cybersecurity must become the fourth-most highly critical objective for maintaining OT environment systems, alongside system resiliency, safety, and reliability.

Associated Drivers

- **Cyber insecurity:** Theft, cyberattack, and negligence create a crisis of digital trust
- **Reimagining the material world:** Revolutionized processes expand technology reach
- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors

IT Impact

- Chief information security officers and other IT security leaders must communicate risk and have a two-way dialogue with those who manage operational technology environments.
- Security must not be a disruptive influence on OT environments. Traditional security products, such as intrusion prevention systems and firewalls that can be deployed and fully functional for IT environments, cannot function as effectively in OT environments because of a broad range of industrial protocols and the critical need for zero false positives.
- Scalability and extensibility must be critical factors for security technology buyers. Security solutions should be capable of supporting hundreds of assets without requiring additional hardware. Alerts generated by these devices must be easily digestible for security operations center personnel with enough context for OT engineers to gauge the risk and quickly conduct a thorough investigation and apply remediation actions if necessary.

Guidance

- Establish an ICS security triage team consisting of all the key stakeholders that understand established processes and typical workflow. It should include all necessary operational technology personnel and key business stakeholders.
- Assess internal processes for tracking IoT device assets, associated recalls, security alerts, and other manufacturer communications. Patching policies and processes should be clearly communicated to asset owners to avoid delays and disruptions.
- Create a baseline of normal device and sensor behavior to identify anomalous activity that could be an attempt to manipulate the device or the data it is collecting and transmitting.
- Introduce a digital-focused security practice that can address cybersecurity concerns.

Prediction 2: By 2024, 50% of Manufacturers Will Network Related Product and Asset Digital Twins into Digital Twin Ecosystems for a Systems-Level View of Their Business and 5% Reduction in Cost of Quality

Digital twins, or virtual representations of products and assets, can be used to manage multiple aspects of a manufacturing business, including highly complex, customized products and connected assets, such as manufacturing plants or facilities and the assets within them. Data and processes from multitier supply chains, service plans and execution, and the operating environment perpetually feed digital twins to ensure the most up-to-date view of the past, current, and future performance and condition of products, assets, facilities, and plants.

Digital twins are being used in fixed asset-intensive industries like oil and gas and utilities to operate individual assets and model asset performance within the collective asset of the plant. These are the

early stages of digital twin ecosystems, where virtual images of related assets are continually monitored and optimized. Engineering-oriented companies like automotive and aerospace, as well as technology-oriented companies like high tech and semiconductor, will be next to move to this approach as the velocity at which they need to respond to demand and manufacture products is increasing exponentially. As demand shifts or ramps up and customer needs and requirements change, manufacturing assets and processes need to be flexible and dynamic, and digital twins for related and interrelated digital twins are a tool to enable this.

These fixed assets in a plant or facility, as well as mobile assets such as automotive or heavy equipment fleets, also need to be modeled and validated quickly and accurately so time-to-market goals are met. For automotive and heavy equipment companies with vehicles that will be autonomous ready in 2021, the multiple digital twins of each vehicle can be used to monitor and optimize performance and ensure functional safety within their environment – city, town, mine, or construction site. This is the next stage of digital twin maturity, brought to life through simulation and Internet of Things, where multiple digital twins of assets and their relationship can be viewed and managed through ecosystems of digital twins. That said, it's important to remember that digital twins can be data rich, complex, and networked, as well as lightweight for ideation and collaboration – essentially a visual, digital container of information that flows across the NPI process. Apply digital twins using a scale of complexity need, where they can support this simple collaboration and communication, up to operation of networks of digital twins.

Associated Drivers

- **Sense, compute, actuate:** Turning data into value
- **Reimaging the material world:** Revolutionized processes expand technology reach
- **Next chapter of DX:** Technology-driven transformation altering business and society

IT Impact

- There will be a need to manage the influx of data from connected products and assets, as well as for ongoing application development.
- You will have to invest in the latest simulation and application development software tools in your organization to ensure fidelity of the product or asset model along the related life cycle.
- The security protocols, authentication, and threat detection technologies will have to be in place to keep the ecosystem of digital twins secure.
- There will be a need to foster collaboration between IT and OT groups as these two worlds continue to converge – IT can help OT align with business systems and OT can provide IT with operational knowledge and support.

Guidance

- Consider the operational and organizational changes that may need to take place as you deploy digital twins and become a data-driven manufacturer.
- Focus on areas of your business that have potential to scale across equipment, sites, or technologies.
- Establish a closed loop through digital twins: rewind and fast-forward product and asset performance information to learn from past issues and predict and optimize future performance.
- Identify revenue growth opportunities by adding value to existing offerings or through the creation of new products/services.

Prediction 3: Despite Supply Chain Complexity Hindering Innovation, 50% of Manufacturers Will Have Implemented Predictive Field Services Across Connected Assets to Improve Delivery Speed and Customer Value by 2024

Manufacturers no longer have the luxury of maintaining the status quo as it relates to delivering service to the equipment and products they sell to customers. Competition is a major factor driving decisions and investments in technology to support improvements in field service delivery. In IDC Manufacturing Insights' 2017 *Product and Service Innovation Survey,* the top factor driving investment in service efforts was a desire to more quickly respond to product quality issues and customer complaints because of increased competition and escalating customer expectations for better service. This need to deliver faster service demands that manufacturers rethink old service models of efficiently reacting to issues.

Historically, reacting to a customer call for service was adequate and manufacturers primarily needed to get more efficient at reacting faster. This is no longer good enough as customers understand that manufacturers have the data on equipment to deliver service in advance of a failure as opposed to the customer triggering a service event. Despite having the data to transform, field support is still quite reactive. The chasm between reactive and predictive field support has not closed as data flows from the equipment sits in databases cut off from the service organization. This problem is exacerbated as networks of partners, dealers, third-party service teams, and customers become more complex and as these stakeholders leverage different tools and systems that often do not or can't talk to each other.

IDC believes that to predictively deliver field support and resolution, manufacturers need to shift from a focus on connecting assets and predicting health to an external ecosystem focus that connects partners and service teams.

Associated Drivers

- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors
- **Sense, compute, actuate:** Turning data into value
- **Next chapter of DX:** Technology-driven transformation altering business and society

IT Impact

- To move from a reactive service model to a more predictive model, IT must ensure field service leadership has access to real-time data captured on equipment and products.
- The IT culture needs to adopt a service- and customer-first mindset to enable tools that are specific to the challenges of delivering predictive and preventative field support.
- IT needs to enable a seamless flow of data across the enterprise to ensure silos of information are not a hinderance to the field team's ability to predict service needs and the resources available to solve those problems.

Guidance

- Provide access to product and equipment performance data with service leadership and the field service team in real time via mobile tools to ensure resources can be allocated prior to failure.
- Invest in machine learning (ML) and artificial intelligence (AI) capabilities to better predict outcomes and future performance levels of assets and products across the service supply chain.
- Educate and train customers and partners to the value of predictive service to highlight the impact and opportunity while rationalizing the increased costs associated with this transformation.

Prediction 4: By 2020, the Success Rate of AI Implementations in IoT Will Have Reached 90%, with the Major Factor Behind this Success Being Collaboration Between Data Scientist and Engineering Teams

The evolution to machine learning is accelerating in IoT projects. According to IDC's 2017 *North America IoT Analytics and Information Management Survey,* 31% of the respondents who deployed an IoT analytics solution used machine learning. In addition, usage of machine learning more than doubled for respondents that were actively developing an IoT solution at the time of the survey. The most common use case for machine learning in IoT is for predictive analytics, with 83% of the respondents developing predictive analytics capabilities.

Despite the strong level of interest, ML today is an emerging technology with a scarcity of skilled professionals able to use the technology effectively. The most common options for enterprises building their own IoT solutions that require ML are to:

- Leverage on-staff data scientists placed horizontally in enterprises as a shared service.
- Outsource model building to data scientists who are part of a professional services team.
- Experiment directly with open source ML models.

IoT predictive analytics is effective only when predictions point to a cause and its effect. Often the initial runs on ML have low causality, which means teams abandon the ML efforts or have no ability to act on the prediction. As more engineers across domains — mechanical, electrical, software, and systems — take the classes required to train on machine learning, IoT predictive analytics management is likely to shift to the engineering teams. This will particularly accelerate as the next generation of engineers depart university, armed with classic engineering skills and knowledge, combined with AI, ML, and data analytics capabilities as well. Meanwhile, successful efforts involve close partnership between the types of skills that are required to deliver usable IoT analytics. For most organizations, this will be realized through close collaboration between hired data scientists or service partners, the head of engineering or R&D, and designated engineers.

Enterprises may decide to choose commercial IoT analytics applications that incorporate ML. But for those that need to build their own algorithms, successes over the next few years will involve partnering between data scientists and engineers as they work together to incorporate known conditions and additional sources of data to improve the outcomes. This approach will ensure that optimal, accurate options are presented to engineers to aid in decision making during business planning, engineering changes, or new product introduction.

Associated Drivers

- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors
- **Sense, compute, actuate:** Turning data into value
- **Next chapter of DX:** Technology-driven transformation altering business and society

IT Impact

- Data scientist teams will need to work jointly with the engineering team to construct data and models that make sense. That may require a process change to ensure that the entire team working on the project accept the results of the effort.
- IT will consider a more agile development process as teams improve the algorithms and data sets as problems are identified with the model.

- IT needs to create a champion challenger structure within the platform they choose to run IoT analytics to test the performance of improved models before they move fully into production.

Guidance

- Include problem detection, which monitors streams of data against rules with known conditions to detect problems as early as possible, in phase 1 of IoT analytics if not already implemented.
- Introduce data scientists alongside the engineers and operations teams. Once condition-based monitoring is established, the goal is to meaningfully improve early detection using ML.
- Turn to the use of ML and other optimization tools, as your organization's deployment matures, to determine next best actions aimed at augmenting and possibly automating decision making. The system should be able to trigger actions or recommendations in the appropriate enterprise applications.

Prediction 5: By 2020, Over 30% of IoT Initiatives Worldwide Will Fail to Demonstrate a Clear ROI, with Organizations Lacking the Necessary KPIs to Monitor Progress from the Early Stages of Such Projects

Amid the digital economy, organizations have been keen to test the multitude of technologies promising a glimpse of a competitive advantage against their peers. IoT has been no exception, with over a third of organizations worldwide currently involved in IoT trials and pilots and a further 30% planning to invest in the coming months. Yet limited IT budgets find themselves spreading thinly across all these multiple technologies, making it necessary to monitor the success of the individual projects. Hence, the need to prove clear results from past investments becomes crucial to ensure new budget for future initiatives. In addition, organizations need to be able to benchmark themselves against their competitors to understand their positioning in a rapidly changing market.

Technology users need to be able to prove the impact of their IoT projects to company results — yet demonstrating a ROI can be challenging if a concise set of KPIs is not available to show the evolution and impact of the initiative. End users must be able to monetize their IoT investments in a variety of ways: from ensuring an impact on the company top line and cost structure, by improving operational efficiencies; contributing to product and process innovation; and helping create alternative lines of business because of the insights and data gained through the IoT sensors deployed.

Yet monetizing on existing IoT deployments requires careful consideration of the set of KPIs to be monitored throughout the lifespan of the initiative, as well as understanding the potential reach of the project outside its immediate area of deployment. Examples of potential KPIs looking beyond the immediate area of implementation could vary from standard financial metrics (such as bookings, revenue, and profit margin), product/service innovation metrics (patents, R&D activity), customer and employee satisfaction metrics, or revenue generated directly from the data captured by the IoT sensors, to name a few.

Identifying those potential KPIs and extended reach of a given IoT solution can be difficult during the planning and early stages of an implementation or pilot, partly due to short-term visibility of the solution and the objectives it is trying to achieve, partly to a lack of exposure during the pilot phase to other areas in order to identify potential impact elsewhere in the organization, and partly due to the limited understanding of the technology and its potential consequences and reach that technology users may have in the early stages of adoption. IDC believes that over 30% of worldwide IoT initiatives will still fail to identify and monitor these KPIs by 2020, leading to an inability to prove its impact in the wider organization and hence securing additional budget to either continue the initiative or replicate throughout the organization.

Associated Drivers

- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors
- **Sense, compute, actuate:** Turning data into value
- **Reimagining the material world:** Revolutionized processes expand technology reach

IT Impact

- IT departments unable to demonstrate the clear impact of specific IoT initiatives will find it difficult to secure additional budget for future initiatives, failing to concentrate resources on those areas having the greatest impact on the business.
- IT will risk identifying potential new areas of growth or new revenue lines by failing to establish the correlation between the IoT projects and all other areas of the business.

Guidance

- Coordinate actions and establish clear joint objectives with other areas in the organization from the early stages of inception, before IoT projects reach even the pilot stages.
- Agree on specific measurements and KPIs across IT and lines of business (LOBs) and monitor them continually to discern which initiatives are generating a clear ROI and are capable of monetization and which ones can be discontinued. This allows the organization to focus resources on those demonstrating clear results. Evolve KPIs with time as the nature of the business and its needs develops.

Prediction 6: With 40% of Initial IoT Data Analysis Occurring at the Edge by 2022, Organizations Will Invest More in Gateways to Aggregate and Analyze Edge Data, Especially in the Context of IT, OT, and CT Systems

IoT is a key DX initiative. It enables firms to obtain valuable insights from data collected via networks of connected devices (beyond computers, laptops, and smartphones). IoT enables firms to digitize and better control the "things" they rely on to conduct business. IoT is not isolated to a single industry or use case. Firms in industries such as transportation logistics, healthcare, hospitality, insurance, manufacturing, and retail are already taking advantage of IoT to gain greater efficiency, rapidly go to market with new products and services, develop new customer engagement models, and enhance customer experiences. Much of what firms can do with IoT is centered around the data they get and the resulting control and actuation (action) of the "things." Data in turn is forcing a kind of transformation within industries — the emergence of edge computing and the convergence of IT and OT.

IoT gateways enable firms to perform the first layer of data aggregation from IoT sensors. They can run compute activities that involve analyzing, transforming, aggregating/summarizing data, or monitoring data, as well as any activity that makes decisions, creates new data, and alerts or informs end users or other systems. They can also carry out network functions such as managing and collating endpoint to core traffic and/or aggregating data from distributed devices and sensors in a local environment. Converged IT, OT, and CT systems enable firms to build an intelligent edge, by providing the ability to analyze data collected by the gateways at the edge. They are designed as ruggedized general-purpose systems with datacenter-grade industry-standard computing hardware and integrate OT functions such as control and data acquisition systems. Many of the IT functions such as data analytics require significant computing resources.

The ability to push the initial aggregation and analysis of data (inferencing, and some amount of training) reduces the time to value for IoT-related data. With faster insights, the ability to act is far more superior and timelier relative to a centralized control and actuation model.

Associated Drivers

- **Next chapter of DX:** Technology-driven transformation altering business and society
- **Platforms, platforms, platforms:** Industry competes for innovation at scale
- **Sense, compute, actuate:** Turning data into value

IT Impact

- The boundaries of compute no longer limited to the datacenter (They stretch all the way to the endpoints, and selecting an appropriate computing platform, along with connectivity and data persistence, must be part of an IT strategy for the edge.)
- Managing asset sprawl and deploying and managing IT, OT, and CT apps along with the various hardware platforms
- Managing ephemeral and persistent data to be collected and analyzed, while the devices it resides on are operated within the service-level objectives agreed upon with the business
- Managing physical device, user, application and data security, and governance like the core datacenter

Guidance

- Consider a cloud-first model for development and deployment of IoT-centric applications. The selection of components of a distributed edge (gateway) infrastructure depends on the kinds of functions that will be performed there. This model drives the ability to utilize dispersed assets and services within a core-edge infrastructure topology.
- Create a data flow and action control paradigm for compute and storage infrastructure. This strategy allows IoT infrastructure to span from massive datacenters at the core to micro-datacenters and intelligent devices in critical edge locations. The right type of edge infrastructure provides the basis for which OT functions can be software defined or run on separate infrastructure.
- Implement processes for data governance, centralized compliance controls, and risk management. Firms need to make their environments compliant from core to edge and build dynamic risk management frameworks that can identify and adjust to changing threats.
- Adopt advanced analytics and insight capabilities. This enables firms to analyze and gain insight from large data sets and have the future vision to reduce the complexity while accelerating prescriptive action from analyses.

Prediction 7: In 2019, Blockchain's Limitations in Processing Vast Numbers of IoT Transactions in Real Time Will Limit IoT Integration into Blockchain and Thus IoT-Related Spend to 5% of Overall Blockchain Spend

Blockchain presents a wide range of possibilities in terms providing a faster, safer way to verify key information, exchange value, and establish trust. However, when considered in tandem with the IoT, it is important to pragmatically consider how blockchain and IoT will coexist in the near future. There is a sense that the decentralized nature of IoT and blockchain complement each other, but providers of blockchain applications are still standing up their offerings and organizations are just experimenting with blockchain use cases.

This limited adoption directly relates to blockchain limitations around handling multiple transactions at the moment. In some financial use cases, where transactions happen at a modest cadence, blockchain's capabilities are already beginning to show some promise (e.g., cross-border payments, internal accounting applications). But when looking at the Internet of Things, where tens or thousands of connected devices will be generating one or many transactions in real time, blockchain technologies are still not up to task. The processing power of a blockchain transaction can be compute intensive even in permissioned implementations. That will make it difficult for blockchain technology to handle the streaming of data from IoT applications. The latency and the processing required to move data through blockchain is still too great to support IoT use cases at scale. This is especially worth remembering as blockchain vendors tout their technologies in critical use cases such as healthcare or transportation.

Although the reality is that we are still a long way off from having a blockchain-powered IoT, anticipated improvements in processing capabilities and the potential for combinatorial benefits will mean that over time the two technologies will become more intertwined.

Associated Drivers

- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors
- **Platforms, platforms, platforms:** Industry competes for innovation at scale
- **Next chapter of DX:** Technology-driven transformation altering business and society

IT Impact

- IT will have to invest time and resources to understand the various blockchain platforms (i.e., Ethereum, Hyperledger, R3 Corda) and services to determine which one meets the needs of the organization and the use case.
- The latency issues of processing transactions could mean that blockchain is not an ideal technology presently to track or monitor an asset as it moves through a supply chain, for example.

Guidance

- Look to engage on IoT projects that include blockchain on a very small scale and are proof of concept. As the technology develops further, the pairing of IoT and blockchain will be more symbiotic.
- Ensure that the lead use cases for IoT and blockchain can be found in supply chain applications, asset management, or applications that reduce risks be it physical, financial, or reputational fit with the business problem your organization is seeking to solve.
- Participate in communities supporting blockchain's evolution and development. Every blockchain platform has an eager and engaged community sharing information, data, and code to companies experimenting with the technology.

Prediction 8: By 2020, 70% of Organizations Will Leverage Commercial IoT Platforms to Develop and Deploy IoT Applications, and More than 50% Will Have Multivendor IoT Platform Environments

IoT platforms provide key pieces of functionality needed to develop and deploy an IoT application, such as the middleware services for bidirectional device communication and message capture, security, device and data management, and analytics. In theory, a single platform should offer a common way to develop and deploy all IoT applications across the enterprise, leading to faster and more secure

application development. In reality, IoT environments are highly variable and complex, leading to a situation where a single platform may not suit the needs of all use cases across an organization. With the 2017-2018 *Global IOT Decision Maker Survey* highlighting that only 36% of IoT project decisions are made by IT, many platform decisions will be made on a project basis by a line of business, instead of on a horizontal technology basis. Given these trends, we believe that within at least 50% of organizations that have deployed IoT projects, more than one IoT platform is currently in use.

In IDC's *Global IoT Decision Maker Survey,* 57% of respondents with current or near-term IoT projects were leveraging commercial IoT platforms for their projects; a further 35% were planning to use a commercial IoT platform at some point. Therefore, it is reasonable to believe that this percentage will grow to approximately 70% by 2020. While do-it-yourself point solutions will continue to be leveraged for experimentation, we believe that once companies reach production scale, the need for commercial support and partnering will drive the move to platforms.

Associated Drivers

- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors
- **Platforms, platforms, platforms:** Industry competes for innovation at scale
- **Sense, compute, actuate:** Turning data into value
- **Reimagining the material world:** Revolutionized processes expand technology reach

IT Impact

- Although the platform buying decisions are often at the business unit level, LOBs will come seeking help from IT when they need to scale the system, leading to additional burden on IT staff.
- The multiplatform syndrome will lead to IoT data siloes, making data management more complex and increasing the chances of a security breach.
- In situations where a multiplatform approach is necessary, IT will need to build an integration layer on top of the various IoT platform databases to provide a holistic view of IoT data.

Guidance

- Develop an IoT center of excellence so all key stakeholders (LOB, IT, and others) are looped into IoT platform purchasing decisions.
- Vet all IoT platform purchasing decisions for the fit with the IT existing architecture or their vision of where the enterprise architecture is moving to.
- Involve IT in all IoT projects from the earliest stages, so they can test the scalability of the system, understand how IoT data will integrate with IT data, and vet the full chain of trust for the IoT data from the endpoint to the cloud or core.

Prediction 9: By 2021, 45% of Video Surveillance Content Will Be Used to Provide Context to Data from IoT Endpoints in Public Safety Scenarios and in Transportation Hub and Campus Monitoring, Among Others

One critical, and emerging, input to the IoT is video. Video provides valuable visual data to augment other sensor data and inform decisions. Coupled with computer vision and artificial intelligence, we can "see" more than was ever thought possible – faster and more accurately – from video. It is also the place where the edge compute comes into play. The video paradigm is growing increasingly important in IoT environments with high-security requirements and low tolerance for network latency or IoT environments that may have intermittent access to connectivity. A video surveillance camera or video

sensor on a machine will collect and process data especially in scenarios where real-time response is required such as real-time traffic or intelligent traffic redirection.

Yet video is not only an endpoint to manage itself but can provide critical context to the environment around it, including other IoT sensors within its purview. Progressively, IT and OT are merging. With card readers, elevators, and other OT assets are being connected to the network, organizations are eager to integrate these data feeds with video surveillance solutions. For those organizations looking to manage all their endpoints seamlessly to help provide a linkage between IT and OT, video can play an important role. They are looking to have other IoT endpoints work in concert with the video systems to provide a full picture of the IT/OT infrastructure.

Associated Drivers

- **Sense, compute, actuate:** Turning data into value
- **The race to innovate:** Speed of change, delivery, and operations separates thrivers and survivors
- **Reimagining the material world:** Revolutionized processes expand technology reach

IT Impact

- The increasing use of video to capture and process data is putting increased strain on compute, storage, and network resources.
- Video generates massive amounts of data. Unless an investment in computer vision or other AI technology to help process and interpret all the images and associated content, it will be difficult to see a quick ROI of investing in a video surveillance solution.

Guidance

- Consider investing in a video surveillance solution to help manage your IoT assets, and look to a partner that offers an open, integrated and holistic platform approach to support their video surveillance solution.
- Consider how video surveillance can provide important context – or cost savings – for other IoT sensors by providing a visual rendering of key metrics or behaviors of other endpoints.

Prediction 10: By 2022, Problems Aggregating and Rationalizing Sensor Data into Actionable Insight Will Have Forced 20% of Large Manufacturers to Insist on OEM Data Being Reconciled in IoT Data Exchanges

The number of deployed sensors is expected to exceed 80 billion worldwide by 2025. Though many of these will contribute only small amounts to the overall data sphere, the billions of devices spending over 90% of their time delivering data means that data environments (which have been predominantly read oriented) must now deal with a continuous influx of data. An obvious feature of sensors, regardless of their purpose, is that they can share information effectively with the outside world. This information can be mission critical (e.g., obstacle warnings) or not (e.g., temperature and humidity readings), with different bandwidth requirements (from very small data points up to video streaming) and different latency needs (from batch up to real time).

IDC expects to see in future a platform-driven data market based on information generated by all classes of sensors (from power stations to vehicles to animal trackers), transmitted over a variety of communication protocols (from satellite to cellular to low-power WAN), depending on the application. This data will not necessarily come from one vendor nor in one consistent format. IoT use cases will, by necessity, utilize wide-ranging ecosystems of providers, where some data will come from sensors

owned by the enterprise (in a factory or warehouse – this is likely to be the minority situation) and where others will come from vendor/provider-defined data sources (a vehicle or elevator with in-built sensors and data formats) to purchased data sets (such as weather, traffic flows, and congestion).

Having access to such rich sets of data allows for richer and deeper insights. Integrating those data sets in an effective time frame in a manner that delivers consistent views derives insight into enterprise behavior and supports the sharing of data and insights among multiple interconnected stakeholders. This will enable features such as optimized supply chain planning; production management; retailer insights based on weather, time of day, and seasonality; travel experience customization; smart maintenance; and connected fleet management.

The benefits delivered by an interconnection platform – such as security, high performance/low latency, private connectivity, and any-to-any connectivity – can help enterprises solve their challenges and enable new developments within the industry. However, the level of complexity, security, transparency, and scalability that this model requires, as well as compliance considerations, makes it difficult for enterprises to go it alone and highlights the significance of increased collaboration with other industries to extend the breadth of choices for customers. Hence IDC predicts that by 2022, problems with aggregating and rationalizing OEM sensor data into time series will force 20% of large manufacturers to insist OEM data is reconciled in IoT data exchanges.

Associated Drivers

- **Platforms, platforms, platforms:** Industry competes for innovation at scale
- **Sense, compute, actuate:** Turning data into value

IT Impact

- Ecosystem participation requires massive data sharing and collaboration.
- Data management skills is essential for those who wish to consume data arising from sensors, by being transparent about what they collect and how they use it, by working on an opt-in basis, and by leveraging open platform concepts.
- Understanding the timing, volume, and transformation needs of data sets, whether owned or acquired, will become an expanded responsibility as business users demand faster and larger data sets to drive decision making.
- To deliver trusted data sources, IT departments will have to learn how to rely on innovative principles for data authentication such as blockchain and distributed ledger.

Guidance

- Inventory data sets from owned and acquired sources along with the platforms they reside in to understand integration needs to support these growing demands.
- Evaluate emerging alternatives based on interconnection platforms that may help in implementing the changes required to deliver the coming sensor-driven data revolution.
- Consider appointing a chief data officer (CDO) to champion the change and to lead the strategy and road map.
- Avoid being locked into systems that may fall short of interoperability and scalability needs that may only become apparent as the data requirements and analytics business grows.

ADVICE FOR TECHNOLOGY BUYERS

IoT is increasingly becoming a foundational element of any next-generation technology investment as its reach is seemingly infinite. Looking ahead to 2019, the IoT is entering its next chapter and several intersection points with other emerging technologies are becoming evident. With this in mind, IDC's IoT team believes the following actions are critical for CIOs and decision makers to keep top of mind about their IoT investments in the coming year ahead:

- **IoT and security.** Establish an ICS security triage team consisting of all the key stakeholders that understand established processes and typical workflow. It should include all necessary operational technology personnel and key business stakeholders.
- **IoT and digital twins.** Consider the operational and organizational changes that may need to take place as you deploy digital twins and become a data-driven manufacturer.
- **IoT and field service.** Educate and train customers and partners to the value of predictive service to highlight the impact and opportunity while rationalizing the increased costs associated with this transformation.
- **IoT and artificial intelligence.** If not already implemented, phase 1 of IoT analytics should involve problem detection, which monitors streams of data against rules with known conditions to detect problems as early as possible.
- **IoT and ROI.** IT and line of business will need to agree on specific measurements and KPIs, ensuring their ongoing monitorization to be able to discern which initiatives are generating a clear ROI and are capable of monetization and which ones can be discontinued, allowing the organization to focus resources on those demonstrating clear results. These KPIs can evolve with time as the nature of the business and its needs develops.
- **IoT and the edge.** Advanced analytics and insight enable firms 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. Edge gateways are increasingly being used for IT analytics based on the data the OT software collects. With accelerator technologies, such as GP-GPUs and FPGAs, edge gateways can participate in training and inference functions more effectively.
- **IoT and blockchain.** Ensure that the lead use cases for IoT and blockchain can be found in supply chain applications, asset management, or applications that reduce risks be it physical, financial, or reputational fit with the business problem your organization is seeking to solve.
- **IoT and the platform.** IT should vet all IoT platform purchasing decisions for the fit with the IT existing architecture or their vision of where the enterprise architecture is moving to.
- **IoT and video surveillance.** If looking to invest in a video surveillance solution to help manage your IoT assets, look to a partner that offers an open, integrated and holistic platform approach to support their video surveillance solution.
- **IoT and the data deluge.** Inventory data sets from owned and acquired sources along with the platforms they reside in to understand integration needs to support these growing demands.

EXTERNAL DRIVERS: DETAIL

Next Chapter of DX — Technology-Driven Transformation Altering Business and Society

Description: Digital transformation, the continuous process by which enterprises adapt to or drive disruptive changes in their operations, customers, and markets, has entered the next chapter – multiplied innovation. Now, competition is driven by platforms and ecosystems, and innovation feeds off of itself. Ubiquitous changes affect business in markets, customer expectations, and operational efficiencies, while society sees improvements in daily life. But many businesses are implementing DX without success, and some will fail entirely. Societal impacts include disturbed trust, jobs, alliances, and new inequities. Companies that achieve multiplied innovation can thrive in the next chapter of DX.

Context: In the past few years, we have witnessed the evolution of DX and the disruptions and opportunities it poses for business and society. Organizations of every size and in every industry must adapt to new technologies, new players, new ecosystems, and new ways of doing business. IDC predicts that by 2021, at least 50% of global GDP will be digitized, with growth in every industry driven by digitally enhanced offerings, operations, and relationships. While most organizations are attempting DX, only a small percentage are getting it right. Early attempts are met by subsequent challenges of change management, budget, talent, platform, scale, and sustainability.

The Race to Innovate — Speed of Change, Delivery, and Operations Separates Thrivers and Survivors

Description: Today, survival of the fittest is linked not to size or strength but to the ability to change – to move quickly, adapt, seize opportunities, and be agile. The best-performing organizations – armed with digital-native culture, tools, and processes – are speeding away from the rest, creating a bifurcated and unequal landscape where a few firms exhibit high productivity and profits. The new imperative is to keep pace with business change while increasing the speed of business operations, the speed at which changes are delivered, and the speed and scale of innovation. In an attempt to go faster, many organizations struggle under a legacy of silos and innovations stagnate with redundancy and inconsistency. "At scale" innovation eludes all but the elite few while the distance between thrivers and survivors grows. Some organizations adapt to new models and ecosystems and move from automation to autonomy; others struggle with the basics and fall behind.

Context: Over the past 50 years, the average life span of a company on the S&P 500 has shrunk from around 60 years to closer to 18 years. The rate of change is accelerating dramatically. Time to decide and act requires near-frictionless, fact-based decision-making processes. To thrive, organizations need to be innovating simultaneously on multiple levels (industry change, delivery, operations) at a speed they are not used to. Digital capabilities provide modular plug-and-play technology, business, and industry platforms, allowing businesses to quickly adapt and compete in digital transformation.

Platforms, Platforms, Platforms — Industry Competes for Innovation at Scale

Description: Understanding and building a "DX platform" that can sustain, advance, and scale business and operations may be the most important decisions leaders make for the next 10 years. The platform is the new battleground for innovation, developers, and marketplaces as the industry rushes to enable its customers with a range of platforms. Leaders must discover what their own platform should look like, how they compete in the platform business economy, and what platform vendors they

choose. Megaplatforms compete to own infrastructure and development environments. Application-centric platforms look for the network effect to expand their reach. Industry-specific platforms harness multiplied innovation to build niche ecosystems. Every business must incorporate these new options into its own DX platform.

Context: Today, we are in a platform economy – one in which tools, capabilities, and frameworks based upon the power of information, cognitive computing, and ubiquitous access will frame and channel our economic, business, and social lives. Companies and industries must shift to compete in their own sectors – but also in the new, larger platform business economy. The DX platform concept expands from microservices, technology stacks, and software bundles to PaaS and entirely new digital business- and industry-specific platforms, ecosystems, and operating models. It lies at the heart of digital transformation strategy, providing the architecture that drives and accelerates every digital initiative.

Sense, Compute, Actuate — Turning Data into Value

Description: Today, data and intelligence represent a unique opportunity for creating unimaginable value. IoT, mobile devices, big data – combined with historical data, systems of record, and global information – continually sense an environment and put it into new contexts. Combined with AI and machine learning, organizations are spreading intelligence from the edge to the core to turn data into value. However, it is harder than it appears. Winners are differentiated by the ways they leverage data to deliver meaningful, value-added predictions and actions for personalized life efficiency and convenience, improving industrial processes, healthcare, experiential engagement, data monetization, or any enterprise decision making.

Context: By 2020, in over half of G2000 firms, revenue growth from information-based products and services will be twice the growth rate of the balance of the product/service portfolio. Data as a service (DaaS) presents an expanding market for both providers and consumers. The volume, velocity, and variety of data and the large and diverse data sets create new challenges but, when combined with AI technologies and exponential computing power, create ever-greater opportunities. Any application, process, service, or organization that isn't part, or all, of the new "sense, compute, and actuate" paradigm is missing the boat with digital transformation.

Cyber Insecurity — Theft, Cyberattack, and Negligence Create a Crisis of Digital Trust

Description: Consumers, citizens, and partners have lost faith in technology, creating a crisis of digital trust. Poor technology decisions, human error, or unidentified weaknesses can result in breaches that have a significant impact on businesses and customers. It is even worse when the negligence and hubris of some tech leaders are to blame. On the other hand, new approaches such as security as a service and threat intelligence are proving themselves, and promising new technologies such as blockchain create "trusted transfers of value" and many new opportunities from smart, secure contracts to food traceability. Protecting the security and privacy of an organization's digital assets and the ability to anticipate, identify, contain, measure, and address security risks are critical to mitigating the crisis of trust.

Context: Data breaches, cybercrime, and data privacy scandals regularly hit global news reports. IDC forecasts that global spending on security solutions will reach $120.7 billion in 2021 at a 2018-2021 CAGR of 10.0%. "Contain and control" approaches, augmented with cognitive computing, replace outdated "protect and defend" models. Security initiatives need to employ new technologies and

approaches to evaluate and mitigate the new risks while ensuring privacy, confidentiality, integrity, and availability.

Reimagining the Material World — Revolutionized Processes Expand Technology Reach

Description: New technologies are revolutionizing industrial processes and ushering a "golden age" of new materials. Nano technologies and atomic-level materials create entirely new applications. IoT, robotics, and 3D printing are mainstream technologies in industrial and commercial applications. AI is used to design products that could only be manufactured by 3D printing techniques. Supercomputers are being used to help slice chromosomes and drive the pharmacogenomics revolution. "Generative design" improves strength and removes weight. Technology is driving "de-materialization" – the use of fewer raw materials to produce products and growth – and the obsolescence of outmoded devices and processes in a whole new world of products, production, and materials.

Context: Traditional CAD/CAM vendors and new upstarts are rolling out generative design frameworks, leading to new generations of lighter, stronger products. Genetically targeted drugs and treatments have the potential to effectively combat cancer in our lifetime. New aircraft structures already have significant 3D printed composition, and that's just the beginning. By 2019, generative design and biomimicry will be used by 25% of G2000 manufacturers, resulting in 30% improvement in product development cycle time. IDC forecasts that in 2021, 3D printing investments will exceed $19 billion, worldwide spending on robotics will reach $230.7 billion, and spending on cognitive and AI systems will grow to $52.2 billion.

LEARN MORE

Related Research

- *Critical External Drivers Shaping Global IT and Business Planning, 2019* (IDC #US44330818, October 2018)
- *Worldwide Internet of Things Forecast, 2018-2022* (IDC #US44281718, September 2018)
- *IoT Market Update* (IDC #US44244318, September 2018)
- *IDC's Worldwide Semiannual Internet of Things Spending Guide Taxonomy, Release Version 2H17* (IDC #US43856915, June 2018)
- *Internet of Things: Market Spending and Trend Outlook for 2018 and Beyond* (IDC #US43599418, March 2018)
- *IDC FutureScape: Worldwide IoT 2018 Predictions* (IDC #US43161517, November 2017)

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.

Global Headquarters

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