How AI-Driven IoT Forges New Opportunities

A collaborative research effort between **IoT World Today** | **Cognizant**

IoT World Today | Cognizant

Contents

The automated power of artificial intelligence (AI) is fueling more widespread adoption of intelligent Internet of Things (IoT) technologies, as organizations derive greater insight from massive datasets collected by these devices. With this added insight, organizations get a clearer view of operations and business performance, and can use this data to launch new products and customer services.

For example, AI amplifies the role of IoT in supply chains to improve tracking, traceability and lifecycle management. Machine learning, a branch of AI that enables a computer to gain intelligence without being explicitly programmed, performs real-time analytics on massive IoT data streams to automate exception handling and take informed actions without human intervention.
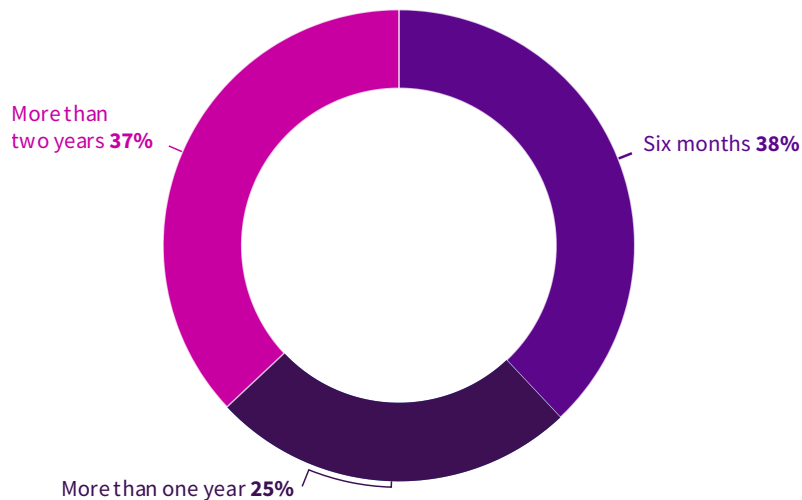
To assess the business expectations of IoT and how AI creates new opportunities, Informa Engage conducted an online survey of executives with IoT implementations planned or underway. The survey, conducted on behalf of **Cognizant**, also explored the challenges faced and found that organizations across a range of verticals, including the industrial sector, are mostly in the early stages of understanding the interplay between IoT and AI.

Another finding is that the need to plan for security requirements was among the leading lessons learned in project implementations. Companies are incorporating AI — in particular, machine learning — into their IoT applications to find insights into the massive data that IoT collects. It's not surprising, then, that a solid majority (71%) of respondents believe that they have much to gain through an integrated IoT and AI strategy.

Fifty-six percent of the survey's 170 respondents are well along with their implementations, indicating they have either integrated IoT across their ecosystem or are now optimized for business value. The remaining respondents are in the early stages leading up to an initial proof of concept. Among the additional lessons learned, more than a third (34%) noted the importance of addressing security, privacy and data entitlement, as well as the need to protect customer data. Also important: the need to establish a clear return on investment (38%).
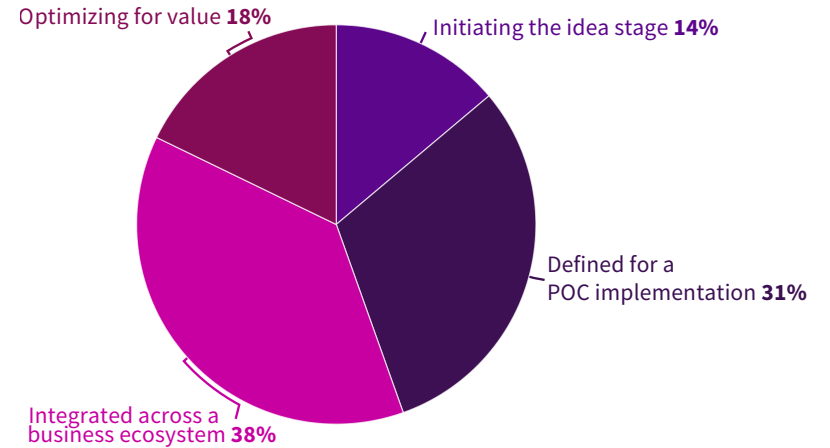
FIGURE 1: Duration & Maturity of IoT Implementations

Duration of IoT Program Implementation(s)

More than two years **37%**

Six months **38%**

More than one year **25%**

Base: All respondents (n=170)

Maturity of IoT Implementation

Optimizing for value **18%**

Initiating the idea stage **14%**

Defined for a POC implementation **31%**

Integrated across a business ecosystem **38%**

Base: All respondents (n=170)
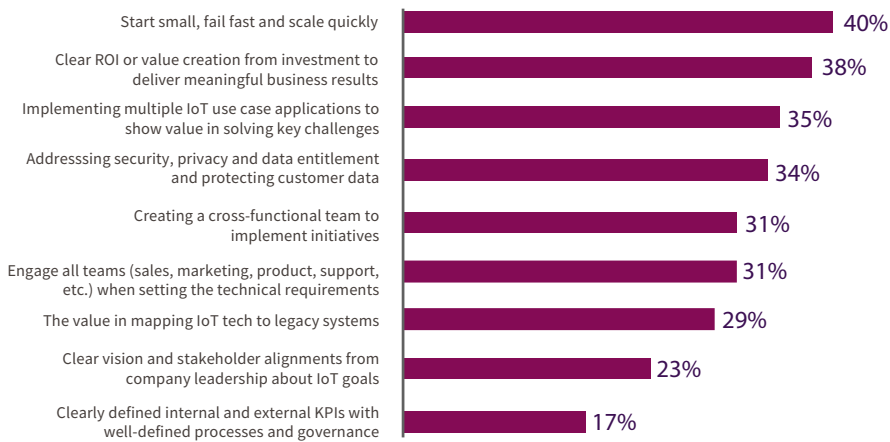
Part 1: Profile of participants

The study sought insight from 170 executives closely familiar with their IoT implementations. The range of job responsibilities included CEOs and other C-suite members (28%) to team leads up to vice presidents (44%) and those in operations, engineering and facilities roles. Represented industries included energy, technology, manufacturing, professional services, and construction and engineering.

Across industries and roles, there was significant agreement on the key lessons learned (Figure 2):

- Start small, fail fast and scale quickly
- Implement multiple IoT uses cases to demonstrate value
- Create cross-functional teams when setting technical requirements and implementing initiatives

Not surprisingly, technology companies are well acquainted with automation (chatbots, vision/image analytics and deep learning) technologies, yet executives from the manufacturing sector indicated they are farthest along with their mapping of IoT technologies to legacy systems. Manufacturers also had more use cases in play and are better optimized for value. By building a factory environment that connects systems and equipment for data collection, manufacturers rated high among the industries for using IoT data for improved decision making, and process and behavior monitoring.

FIGURE 2: Lessons Learned in Adopting IoT Technologies

Lesson	%
Start small, fail fast and scale quickly	40%
Clear ROI or value creation from investment to deliver meaningful business results	38%
Implementing multiple IoT use case applications to show value in solving key challenges	35%
Addresssing security, privacy and data entitlement and protecting customer data	34%
Creating a cross-functional team to implement initiatives	31%
Engage all teams (sales, marketing, product, support, etc.) when setting the technical requirements	31%
The value in mapping IoT tech to legacy systems	29%
Clear vision and stakeholder alignments from company leadership about IoT goals	23%
Clearly defined internal and external KPIs with well-defined processes and governance	17%

Base: All respondents; multiple answers permitted (n=170).

A common manufacturing example is the use of real-time asset monitoring that leads to predictive maintenance, which employs machine learning to assess the status of equipment location, performance, reliability and asset assurance.

Another related use case is remote manufacturing, where sensors track production processes at diverse locations and send status updates to a central control facility that also uses machine learning for machine health monitoring and downtime reduction through failure prediction.
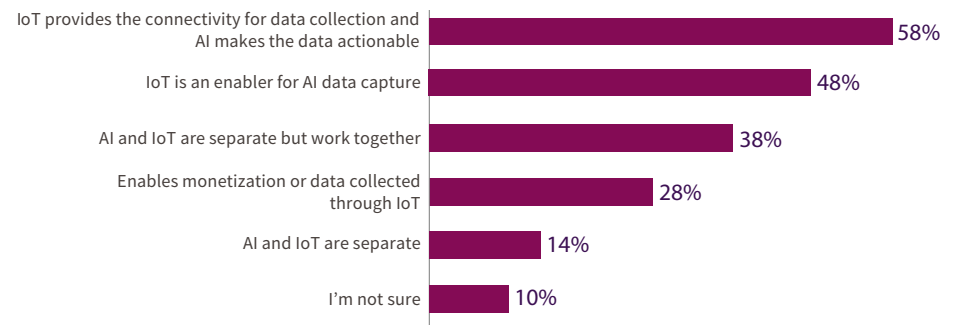
More than half (56%) of respondents are implementing three or more use cases, which may imply that IoT is on its way to advancing business goals of improved productivity and reduced costs, as well as creating new business models.

Part 2: The role of AI in IoT

IoT generates mountains of data, and buried within that data are new insights into organizational or equipment performance and health. AI helps businesses harness the power of IoT by aiding prescriptive and predictive analytics that interpret data collected by sensors, trackers and other input devices. Such intelligent analytics support preventative maintenance as well as improved decision making and forecasting to better serve customers.

Significantly, AI also helps address security issues that IoT implementations might face, as explained later in this report.

FIGURE 3: Perceived Relationship between AI & IoT

| Relationship	%
IoT provides the connectivity for data collection and AI makes the data actionable	58%
IoT is an enabler for AI data capture	48%
AI and IoT are separate but work together	38%
Enables monetization or data collected through IoT	28%
AI and IoT are separate	14%
I'm not sure	10%

Base: All respondents; multiple answers permitted (n=170).

Most respondents have a basic understanding of the relationship between IoT and AI. They were most familiar (58%) with how this relationship helps devices collect data for actionable insights, but less so (28%) in how AI can help to monetize the data (Figure 3). As business leaders further their implementations, we expect their knowledge of applications and benefits will only increase.

IoT, when coupled with AI's predictive analytics capabilities, can drive more accurate decisions across all areas of a business. Nearly half (48%) of respondents understand the role that IoT plays in capturing data for AI applications. IoT enables AI by making relevant and more reliable data capture possible, helping business leaders understand that AI-augmented IoT can support complex decision making with insight gleaned from massive IoT datasets and millions of variables.

While data analytics, forecasting, and informed decisions are established outcomes of AI-driven IoT, using IoT and AI as tools to replace humans is not viewed as a valued benefit, rating lowest among all options (Figure 4). Rather, respondents see the most benefit in ways that improve competitiveness, aid visibility, lower costs and enhance the customer experience.

FIGURE 4: Top Benefits of Combining AI & IoT
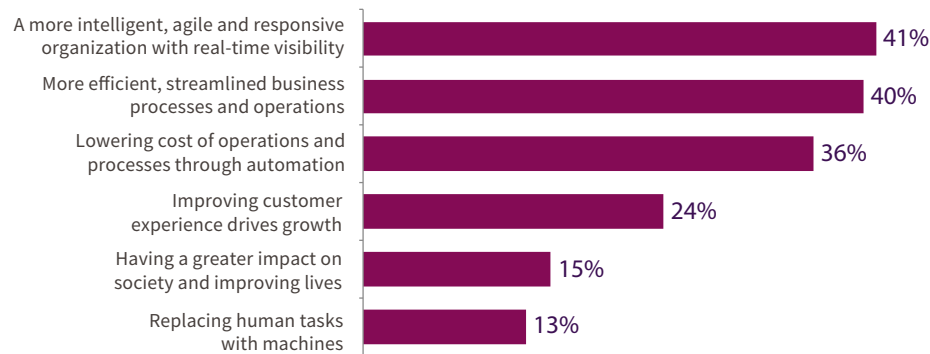
Base: All respondents; multiple answers permitted (n=170).

Part 3: Address potential security threats and data privacy requirements

IoT-connected devices and the data they produce are a potential threat vector that malefactors might seek to exploit if vulnerabilities exist.

AI can be part of the security solution by using machine learning to analyze event data and detect threats before they become critical. A security strategy called security incident event management (SIEM) employs machine learning to process event logs looking for suspicious combinations of events. IoT devices participate by collecting sensor data, including that from access control systems, video surveillance and presence monitors. By feeding this data into an AI-driven SIEM system, businesses gain a force multiplier in the fight against fraud and data loss.

A second role of AI: Ongoing penetration testing, in which IoT networks are continuously exposed to known security threats in order to measure their vulnerability.

By automating so-called "pen testing" and "vulnerability assessment," AI algorithms and machine learning can make these processes more consistent and scalable, culling false-positives and establishing a business' baseline security conditions. Vulnerabilities introduced through human error or software changes are thus quickly identified and remediated.

Part 4: Achieve value and monetization

As with any emerging technology, identifying ways and means to monetize services and products can be a significant challenge. The research shows that more than half of early adopters aim to monetize their AI/IoT transformation by introducing new services, and most of those adopters plan to create new multi-platform (mobile, online or in-person) customer experiences. This provides a path to new business models, as well as more innovative ways to create customer and partner loyalty.

Even industries with more mature AI/IoT experience, such as manufacturing, are using IoT as more than a means to control budgets. For instance, manufacturers use data-driven insights about production bottlenecks to support the design of plants that are more efficient and more effectively IoT-instrumented.

Other sectors exploit new connected products unique to their market segment. In the utilities industry, for example, energy suppliers monetize IoT data by providing homeowners with rebates and rewards to incent reduced power consumption during peak-usage times.

When asked how they monetize their IoT programs, respondents identified several beneficial applications, most of which they apply simultaneously:

- Fifty-two percent are introducing services around connected products
- Forty-seven percent are developing new business processes to optimize operations
- Forty-seven percent are developing entirely new connected products
- Forty-two percent are creating multi-platform customer experiences

Although introducing new services and connected products rank among the top monetization strategies, only 23% are now using these new services and products to identify new customers. When asked how they expect to create value from their analytics, 46% said they will use it to create even more service lines and business models. Organizations might feel their need to focus first on internal processes and their existing customer base before setting sights on using this data to acquire new customers.

How companies create new revenue streams from their IoT programs heavily depends on how they use their data. The findings show much work is needed in this area: only 29% are getting alerts and notifications from sensors, and even fewer (23%) have implemented advanced analytics applications or predictive models.

Clearly businesses must first embrace, rather than discard, the data their IoT collects before they can benefit from it — a process that AI can facilitate. A closer look at the factors that influence the customer experience will show some of the benefits from deep IoT data analysis. Businesses must then use a top-down assessment to fine-tune IoT sensors needed for intended business outcomes.

Part 5: Deploy IoT for an enhanced customer experience

Enhancing the customer experience is a core IoT benefit, because it can help secure revenue streams and boost customer retention. How an organization senses and deploys data collected through its IoT platforms — being mindful of data privacy — can have a significant impact on its ability to fuel growth and monetize data-driven insights.
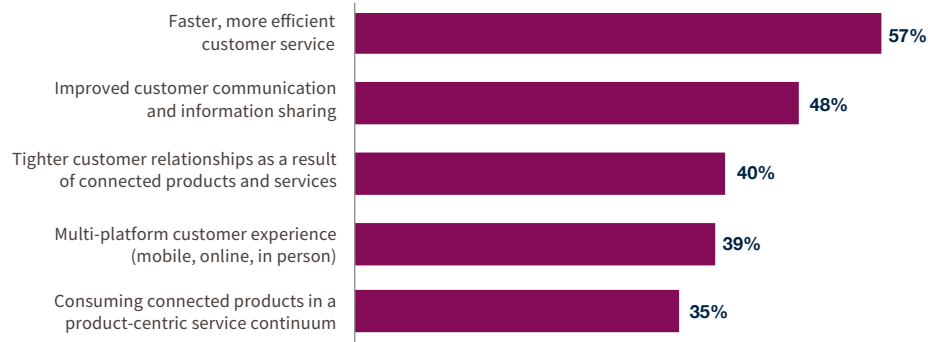
Connected products and services keep customers engaged, making customer interactions more rewarding through such devices as virtual assistants, mobile apps and "smart" services and appliances. Augmented reality (AR), which superimposes computer-generated imagery over a user's view of their real-world surroundings, is the next big thing in AI-driven connected products, with devices already in the market and delivering completely new types of experiences. AR goes far beyond consumer applications to industrial training, troubleshooting and virtual models, called digital twins.

In an era when customers are won or lost based on the experience delivered, 57% of respondents said that if they could further monetize IoT, they would use it to create faster, more efficient customer service, and 48% cited improved customer communication and information sharing as potential revenue enhancers. Forty percent believe that connected products can tighten customer relationships, while 39% envision the value from providing multi-platform experiences. With only 37% of respondents indicating two or more years of experience with their IoT implementation, it might be too early in the lifecycle for many organizations to project financial benefits through improved IoT-supported customer experiences.

Businesses also must not overlook the security aspects of their new augmented customer experiences. Data breaches are not the only vulnerabilities to guard against; already customers are wary of how much data is being collected — and how many conversations are monitored via these devices. As a result, IoT implementers should be security-proactive, with transparent privacy policies and a clear plan for protecting their approach through appropriate network partitioning and monitoring.

FIGURE 5: Value Drivers to Monetize IoT Data and Transform or Personalize the Customer Experience

Value Driver	Percentage
Faster, more efficient customer service	57%
Improved customer communication and information sharing	48%
Tighter customer relationships as a result of connected products and services	40%
Multi-platform customer experience (mobile, online, in person)	39%
Consuming connected products in a product-centric service continuum	35%

Base: All respondents; multiple answers permitted (n=170).

Part 6: Looking forward

As AI and IoT become more commonplace, they introduce implementation challenges. If companies instate AI and IoT without proper preparation, they will likely not realize the technologies' full potential. The best guidance? Keep your eye on the goal of achieving new value.

Companies are right to be concerned about security, so plan to make it an upfront business plan component, rather than an afterthought.

When asked about future plans, less than half (46%) of respondents said they are making operational improvements to enable predictive models. This demonstrates that more work is needed before predictive models become mainstream. The same number of respondents are focusing IoT efforts on creating new service lines, and 39% to support product innovation.

If you're just getting started with IoT, take guidance from the lessons learned by early adopters:

- Start small, fail fast and scale quickly — which requires knowing what data to access. Then, establish a tech foundation to store data, making data complete and clean, and generating intelligence based on what you want from it.
- Identify areas where implementing AI/IoT can improve your business processes and provide a sustainable return on investment.
- Implement multiple AI/IoT use cases to demonstrate value in solving complex challenges across the business.
- Consider security requirements at the start of every project.

Whether your organization is ready for AI and IoT integration depends entirely on how well it has planned. Only by first understanding how the technologies and approaches can be put to work will organizations generate optimal returns for recognizable value.