SOFTEQ

Getting Started with IOT

If you are about to start your first IoT project or you've been on the IoT road for a while, and it's been a rough experience, this book will help you get back on track. It offers tips that you can use to prepare for your IoT projects, and it will assist you in making important decisions, such as choosing a single vs. multi-vendor approach.

If you are considering your first IoT investment, this book elaborates on which IoT solutions are trending up and what to expect in the future.

We've put together this book to help you navigate around the critical aspects of IoT solution development:

- How to set up your IoT project for success
- Some of the common stumbling blocks that can derail IoT projects
- IoT market prospects based on economic factors and technology trends

Inside this E-book

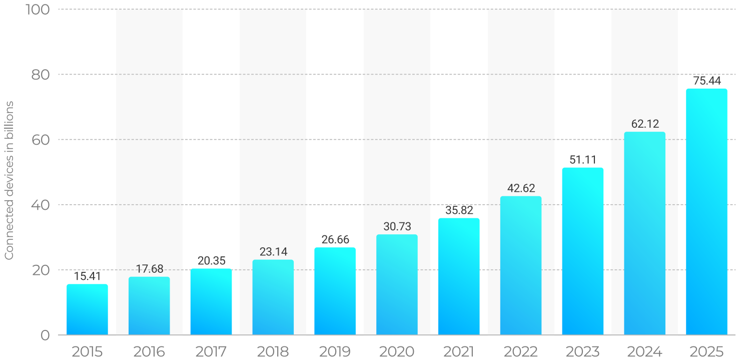
Getting Started with IoT

Why IoT Projects Fail and How to Mitigate Risks

What is IoT?

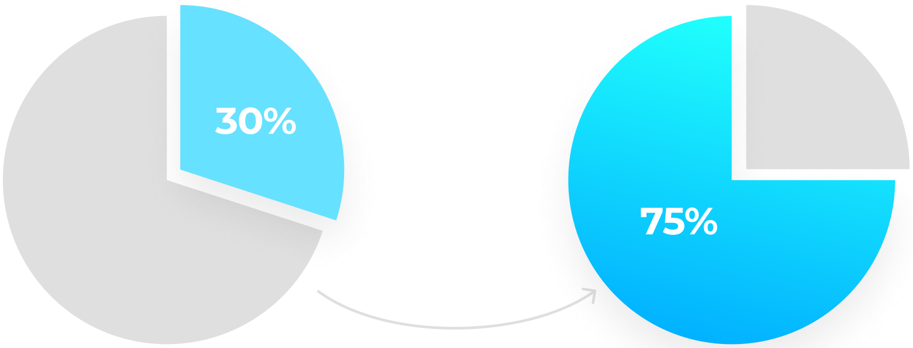
The Internet of Things is a broad term referring to devices and non-electronic objects that collect data from their surroundings and exchange it over the Internet. IoT solutions are used across multiple industries, with consumer electronics, retail, and healthcare taking the lead.

IoT is masterfully making the world a more connected place. The total number of connected devices is projected to reach 75.44 billion units worldwide by 2025. Today IoT is a necessity, not an option. Competition-minded enterprises either adopt a data-driven approach, or drop out of the race.



Source: **Statista.com**

Despite the importance of this technology, many IoT projects fail. A Microsoft survey has revealed that 30% of IoT projects don't make it past the proof of concept (PoC) stage. Among the remaining projects, a whopping 75% fail to deliver on their expected results.



30% don't pass the PoC

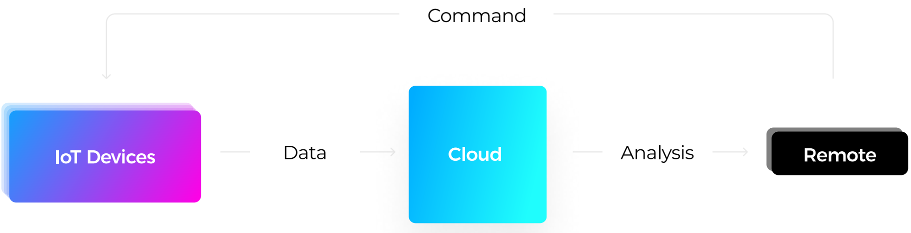
75% of the remaining projects don't yield the expected results

Source: Microsoft IoT Signals report

Why IoT Projects are Prone to Failure

The Internet of Things is a multi-level ecosystem where "things"—i.e., devices equipped with sensors and embedded software—collect miscellaneous data, transfer the data to an on-premise or cloud-based server using secure connectivity protocols, and act on it.

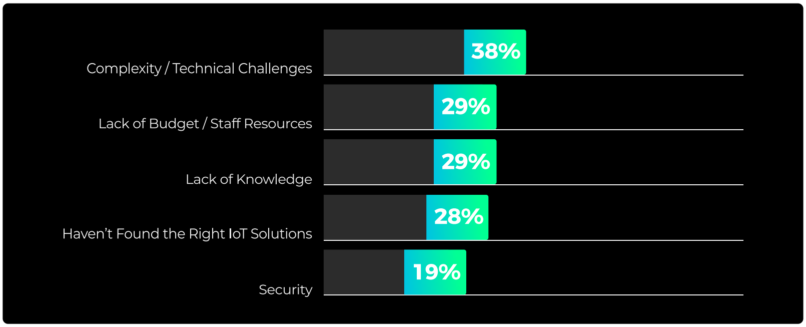
Extra IoT layers include databases and data analytics solutions deployed in the back end, dashboards that visualize historical and real-time sensor readings, and mobile applications, which help users control smart devices and provide anytime, anywhere access to IoT data.



Compared to traditional IT systems like CRM solutions and e-commerce websites, the Internet of Things remains a novel concept. Studies show that 25% of small and medium-sized enterprises (SMEs) are still unaware of IoT and its applications in business. Also, IoT solutions vary in complexity. A brick-and-mortar store where each item is equipped with a printed RFID tag is an IoT solution, and so is a comprehensive telecare system that uses wearable devices to track elderly patients' well-being.

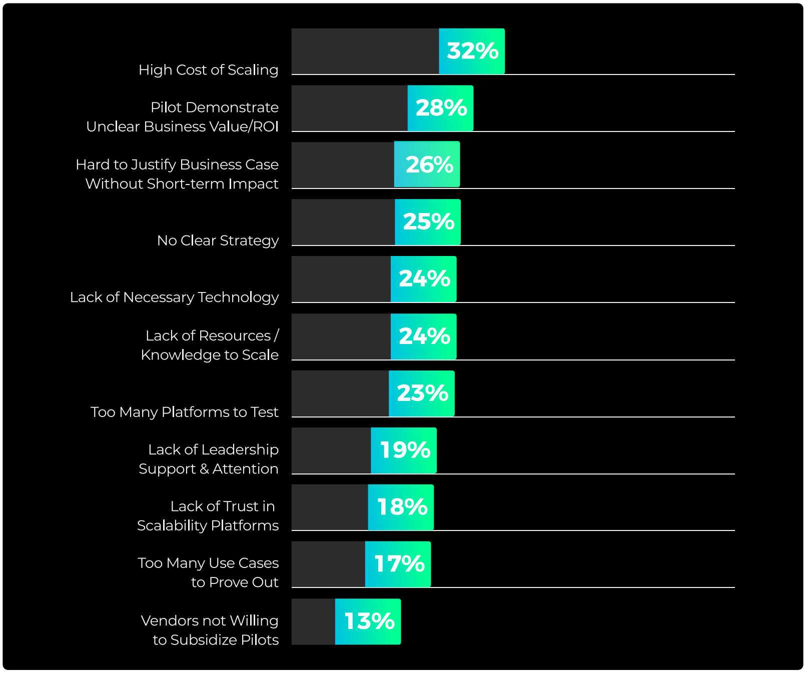
Even large companies with fully-developed IT departments and substantial R&D funds are struggling with IoT development.

According to the recent Microsoft IoT Signals report, 38% of the respondents cite technical challenges as the major barrier to the Internet of Things adoption.



Source: Microsoft IoT Signals

The companies that fail to proceed beyond PoC abandon their IoT projects due to high implementation costs and unclear bottom-line benefits.



Source: Microsoft IoT Signals

8 Tips to Make it through IoT Development

IoT projects vary largely in their requirements and complexity—though common threads can be found throughout. Softeq experts came together to share their advice and experience keeping IoT projects on track in a podcast hosted by IoT for All.

Listen to the IoT for All podcast on how to succeed in your IoT initiatives

LISTEN NOW

> **IT infrastucture, validation, and security are critical erly in your IoT project. Make sure you get them right the first time to ensure your deployment's success!**

Define IoT Solution Requirements

Before you embark on an IoT development project, there are several questions you need to answer:

- What operations and business processes are you looking to automate with the help of an IoT solution?
- What type of a data-capturing device are you going to use?
- Is the gadget capable of running on a proper operating system and processing sensor data locally?
- Where will the data be stored and analyzed?
- What connectivity technologies do you intend to use?
- How are you going to present IoT-generated data to end users?

To verify your idea against your business needs, narrow down the project scope, and outline the implementation roadmap, you should start your project with a Discovery Phase and a Proof of Concept.

In the next step, it is essential to figure out how the system should function—as opposed to what it's supposed to do. This is what IT specialists call "non-functional requirements". The Requirements Analysis phase will help you choose the optimum IoT development technology stack, plan the solution architecture considering the current and projected workload (i.e., the number of users and connected devices), and get more accurate estimates.

Use Case:

One of our clients wanted to create a data analytics platform for packaging manufacturers. The company was looking to install temperature and movement sensors on injection molding machines, send the data to a cloud-based server, and analyze the data to prevent equipment failure and fine-tune the manufacturing process. BLE, ZigBee, and Wi-Fi were listed among the preferred connectivity options.

Following the Analysis phase, the project scope was broken down into several iterations:

- The Softeq team created intelligent sensing devices (ISDs) running on custom bare-metal firmware and conducted field tests to make sure the data is produced in a format suitable for Machine Learning-driven analysis
- The findings helped us refine the requirements for the ISDs
- We chose IEEE 802.15.4 as the primary connectivity standard, which serves as a basis for popular connectivity technologies like Bluetooth, ZigBee, and Z-Wave

- We integrated the devices with AWS cloud services to enable data analysis and visualization

Identify Technology Roadblocks Early in the Project

IoT solutions rely on multiple technology components to exchange data and act on it. These include sensors, devices, embedded software, connectivity protocols, cloud services, and apps. It is often hard to predict how exactly these components will interact with each other and your IT infrastructure.

Use Case:

A fitness jewelry brand turned to Softeq to design a luxury bracelet that would monitor users' physical activity. The device was expected to talk to a mobile application over Bluetooth. However, the company didn't realize the metal case would interfere with the Bluetooth signal. To ensure a stable app-to-device connection, the team modified the radio chip and boosted the Bluetooth signal by 500%.

Make sure that your selected IoT components work together without conflicts.

Avoid Scope Creep

According to the Global Project Management survey, the top three factors contributing to IT projects' failure are erroneous requirements gathering, a change in project goals, and a shift in company priorities. The research also points out that the complexity of a project increases the likelihood of scope creep.

Use Case:

A startup hired Softeq to build a connected dog collar. They wanted to create an advanced pet tracking solution with a GPS module, accelerometer, microphone, and speaker. The gadget and the accompanying cross-platform mobile app would allow dog owners to keep their pets within a safe distance and make sure they get enough exercise.

The ambitious project also called for the battery-powered collar to incorporate five different radio technologies and stream high-definition video over 2G. Because of the numerous feature requirements, the company had some difficulty managing the scope and duration of the project. At the end of the day, the product was shipped, though later than originally expected.

Starting with a minimum viable product (MVP) is an IoT development best practice. This means you first create an IoT solution with just enough features to get buy-in from the C-Suite and show your customers what the new product is about.

Get Your Team on the Same Page

Few companies have the human resources and expertise to create a connected solution under one roof. That's why businesses often have to outsource the development of their functional IoT components to separate vendors—hardware companies, embedded software specialists, and remote mobile and web development teams (we will discuss this in more detail in Chapter 2: How to Set Up Your IoT Project for Success).

Use Case:

A manufacturer of lighting products was looking to upgrade their lighting system. The project involved replacing an RF remote control with a BLE-enabled mobile app. The problem was, the firmware and hardware vendors our client hired had never built BLE-controlled devices before. As a result, the app would not connect to the cloud. Another aggravating factor was the platform choice. Google Firebase, selected as the primary platform for their IoT mobile and web applications, did not work in the location where the firmware development took place, due to local government restrictions.

When outsourcing IoT development, it is best to choose a company that has been engaged in similar projects.

Design Your Solution with Scalability in Mind

Plan your system architecture and choose a technology platform considering the current and anticipated IoT solution workload (i.e., the number of users and connected devices).

Use Case:

Softeq helped a US telecom company optimize the performance of a media streaming solution for digital signage. The system incorporates custom devices that allow advertisers to stream media content on digital displays and collect ad impression data. The reporting functionality was initially enabled through the MongoDB Aggregation Pipeline.

Once the database grew to 20 million records, the system could no longer process user requests and generate relevant reports. To speed up data analytics, the team replaced MongoDB with AWS Redshift. The cloud service helped us do the same amount of data processing and analytics 36 times faster.

While choosing the right technology for your project, think of the anticipated system load

Focus on Security from Day One

98%

of all IoT traffic goes unencrypted

46%

of US companies that make use of IoT solutions have already experienced at least one security breach.

13.4%

IoT-related cyberattacks cost up to 13.4% of total revenue for businesses making up to $5 million annually.

What makes the Internet of Things vulnerable to cyberattacks?

- Embedded software that relies on outdated and unsupported operating system (OS) versions
- Poor hardware design that restricts firmware updates
- Insufficient R&D and testing
- Weak password policies
- Lack of universal IoT security standards
- Legacy software systems, which fail to ensure IT infrastructure visibility and detect compromised IoT devices

Software and hardware-level security vulnerabilities allow cybercriminals to intercept sensitive data or harness IoT devices into giant botnets that execute DDoS attacks and may threaten even properly secured enterprise networks. The consequences of large-scale IoT cyberattacks vary from power grid failures to putting patient safety and lives at risk.

Here's what you could do to avoid IoT security mishaps:

- **Encrypt the data stored on a connected device or transmitted between the components of an IoT solution.** The use of digital certificates (X.509), TLS cryptographic protocols (SSL, TSL), and reliable connectivity protocols (MQTT, CoAP, AMQP, XMPP, ZeroMQ) helps prevent unauthorized access to sensitive data

- **Enhance IoT network security.** For this, you should remove outdated connected devices from your corporate network, implement firewalls, and interface your IoT solution with security monitoring tools: AWS IoT Device Defender, Amazon Cognito, IBM IoT Watson Platform, etc.

- **Reinforce hardware security.** Make sure all sensitive information (personal data, certificates, key, etc.) is encrypted and stored in a secure location, and be sure the device does not install unauthorized firmware updates

Things to Remember

The complexity of IoT projects poses a challenge. But if you clearly identify technology roadblocks, prevent the endless expansion of your project's scope, unify your team, and work with scalability in mind, you will have a better chance to succeed.

How to Set Up Your IoT Project for Success

At this point, you took all the necessary precautions and are ready to start your IoT project. In this chapter, we'll outline when to opt for a multi-vendor approach and how to manage the selected vendors. Moreover, you will learn how business analysts can add value to your team and which problems they can solve.

Choosing between a Multi-Vendor or Single Vendor Strategy

Once you have a clear idea of your IoT project, you will inevitably face the question: who will be your tech partner? Even if you have an experienced and trusted team, they may lack expertise in certain areas or have insufficient human resources to deliver.

However, dealing with multiple providers exposes a product owner to other risks, namely governance-related ones.

The complexity and quick development of the IoT sphere is putting an end to the one-stop shop practice.

Why is a Single Vendor Option not That Attractive Anymore?

A complex IoT ecosystem includes many levels:

- **Hardware level**, where objects turn into "smart things", enhanced with firmware/embedded systems and smart sensors
- **Infrastructure**, where sensor data is stored, analyzed, and processed, be it cloud-based or in-house
- **Mobile application**, establishing a connection between a "smart" object and the project's infrastructure

Let's be honest, it is hard to imagine a software development company capable of delivering such projects, relying solely on its in-house team. Even if you start working with a primary tech partner, soon you may face one of the following situations:

- New requirements come up, and the vendor can’t cope with them
- You need additional manpower to speed up the development process
- You are trying to avoid risks associated with vendor lock-in, etc.

At the same time, many customers are still seeking a technology partner that will take over the development process from A to Z, as this appears more manageable and localized.

That's why the "single vendor vs. multi-vendor" dilemma regularly pops up in the IoT world.

Even when it seems that a single vendor might be sufficient for a particular project, complications and additional requirements can still force you to look for backup.

Disadvantages of a Multi-Vendor Approach

- **Added complexity.** Managing and coordinating different units is not an easy task. When you work with a single vendor, it is logical to assume that the vendor will manage the ongoing processes themself. In case you opt for a multi-vendor approach, you become the coordinating point, managing the cooperation between different teams.

- **Reduced developer collaboration.** At Softeq, we often see situations when communication between the engaged teams is not aligned. As a result, development activities slow down, and vendors start blaming each other.

- **Variations in technologies and process management.** Even if the assigned teams work with the same technology stack, they work with it in their own way. That is why it will take additional time and effort to define standardized rules that all cooperating vendors will comply with, to avoid incompatibility in business processes and technologies.

- **Added costs.** A multi-vendor project is more expensive than a project with a single vendor—at the very least because you have to factor in additional administrative and management costs.

Disadvantages of Single Sourcing

- **Lack of expertise.** As mentioned above, an IoT project is always a complex multi-faceted infrastructure, with a lot of innovative custom solutions in place. In practice, it can be nearly impossible to find a developer skillful enough to manage such a project all by themselves.
- **Limited functionality.** You can hire a great team with outstanding expertise in cloud projects, but their testing team is not that impressive. Or their designers don't live up to the required level. Would you agree to such a compromise when starting cooperation with them?
- **Dependence risk.** Once you work with a single technology partner, you rely heavily on them and it gets harder to negotiate rates and budgets. Additionally, if your partner faces human resources trouble or any other type of misfortune, this will put your project in danger as well.

When does a Multi-Vendor Approach Pay Off?

Going with a single or multi-vendor approach often comes down to the customer's human and financial resources. An experienced IoT development team finds that sometimes choosing a single vendor is the best option, despite the limitations of this approach.

If a customer has already invested resources into product development and now seeks a stable and reliable operating environment, a single vendor strategy would be a winning solution.

However, if a business has enough resources at its disposal, a clear idea about the challenges of a multi-vendor approach, and is ready to manage this complex affair—it will leverage all the benefits of this strategy.

With a multi-vendor strategy you will be getting:

- **The best-of-breed products and services.** When choosing experts in specific domains, you have all the chances to get not just a functional, reliable and predictable product—but something truly innovative and, possibly groundbreaking.

- **Multithreaded work on the project.** When managed right, different elements of the project can be in the works at the same time, accelerating the product development processes.

- **Driving competitiveness**. Working in synergy, vendors are constantly raising the bar of their services and expertise, and the client reaps the benefits from it.

9 Steps for Managing a Multi-Vendor IoT Project

Here is a step-by-step guide for establishing an efficient multi-vendor governance framework:

Step 1: Define the scope of the project

Before delegating tasks to vendors, product owners must assess their project, outline the overall business goals, and how they are planning to achieve them. Without this, requirements will change too often, preventing developers from focusing on the ongoing project. Once you complete this step, you will have a high-level picture of the project vision, the required skill sets for vendors, the technologies to be used, and the main requirements for the success of the project.

Step 2: Select the best tech stack and processes within the allocated budget

Resources are always limited, so it’s best to choose the technologies you can afford right from the start. Let's take a simple example: sometimes it is preferable to opt for the cloud instead of a more expensive server-based solution. This is better than assigning most of the resources to the project infrastructure, while neglecting the upcoming mobile app development or cutting costs on the design.

Step 3: Engage providers

To make sure that everyone is engaged and is doing their job, you need to clearly document the rules. Unify processes and key performance indicators

(KPIs) of each team into a single set of service requirements and optimal performance metrics for each task. You can define this in service level agreements (SLAs). Furthermore, you can ask your selected vendors to sign internal operating level agreements (OLAs), to specify co-working processes among them.

Step 4: Establish the right KPIs

Once you engage a few vendors, it is as risky to monitor too many metrics as it is to do a project with no monitoring at all. Instead, start by figuring out the most critical elements in your project (timely product delivery, compliance with laws and cybersecurity requirements, cost minimization, etc.), and then establish qualitative metrics based on a minimum acceptable required level of performance and quantitative metrics, which would be both realistic and achievable for vendors.

Step 5: Assign roles and responsibility

To minimize functional overlaps and dependencies, each vendor's team needs a clear idea of their individual scope, activities, deliverables, and level of responsibility.

Step 6: Establish a communication and task delegation framework

To manage overflow or workloads, and avoid one team stepping into another's domain, product owners need to supply teams with the rules of how vendors communicate with each other, how they transfer their parts of work, share knowledge, receive feedback and final approval.

Step 7: Encourage the "one-team" approach

Communication troubles are often caused by the fact that different teams have to cooperate on a complex project without knowing each other. Promoting team culture becomes a must, and can be backed up by regular sessions and interactions.

Step 8: Manage risks

A product owner should not only specify the rules and regulations vendors adhere to, but also define penalty clauses for non-adherence. For example, financial guarantees for late delivery or for poor quality deliverables. This will lead to better accountability and ensure that vendors don't pass the buck.

Step 9: Ask for performance reports

To keep track of the performance level of each vendor, you can enforce regular reports, containing updates on progress, accomplishments, and upcoming work.

Benefits of Business Analysis

Business analysis takes an essential place in the entire software development process—and IoT projects are no exception.

Business analysts (BAs) engage with executives and stakeholders to analyze a company's business needs, and carry out a feasibility study to assess the viability of a business idea. They also gather requirements and deliver data-driven ideas that prove the business value of a technology solution.

A detailed business analysis doesn't end with requirements gathering and functionality, it also includes the benefits and value the product poses, along with plausible use cases.

In most cases, BAs work together with the development team throughout the entire project lifecycle.

Such a tandem effort ensures IoT solutions are launched on time, on budget, and up to specification. The task of a business analyst in IoT projects is to clearly define how to achieve coherence between novel IoT technologies and customer expectations, and at the same time drive for operational efficiency and innovation.

Use Case:

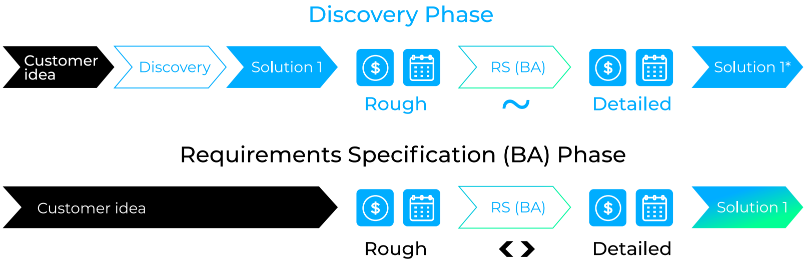
Imagine you are working on an enterprise security system that incorporates connected video cameras. During the development process, you decide to enhance the cameras with object detection capabilities, which require a more powerful microprocessor unit (MCU). This would lead to a complete upgrade of the firmware that enables smart functionality.

The process can push the delivery date indefinitely into the future, as you will have to go through the hardware design stages again. Also, you will have to order new hardware components for trial models (adding delivery time as well), go through the assembly process, test the samples, etc. With business analysis, detailed requirements, and clearly defined use cases, mitigating those risks is not rocket science.

Business Analysis Process Flow

Following the Discovery Phase, customers are expecting to receive market and competitor analysis, a preliminary solution scope, mockups, and a ballpark estimate.

Discovery-Phase vs Business-Analysis Phase



The BA team solidifies the solution's non-functional requirements to analyze how the system should function, prioritizes product features, participates in choosing the optimum tech stack, and prepares a detailed requirements specification that will be used to guide the IoT project development team.

BAs can help your team understand the system's functional and non-functional requirements, prioritize product features, analyze user feedback, and implement the corresponding changes.

Major Problems BAs Can Solve

Problem 1: Misalignment between the problem and a proposed solution

Business analysts double-check if the proposed solution works as expected and determine how it should function by gathering the functional/non-functional requirements.

Use Case:

One of our clients was looking to design a smart dog collar. The collar is a multi-sensor wearable device that helps monitor a dog's location, fitness activity and behavior, and prevent car accidents and straying. One of the solution's functional components is a GPS module to track the pet's location. The BA team was instrumental in determining whether a GPS geofence would be accurate enough, or if the team needed to consider other fencing options.

Problem 2: Targeting an unmanageably broad range of features

BA teams participate in defining the solution scope, tuning the tech requirements, and choosing the most cost-effective approach and tech stack.

Use Case:

The above-mentioned customer wanted to equip their collar with a high-quality camera to track pets in real time. Business analysis showed that it was not feasible. The camera and additional hardware modules were simply too big—the collar would not be compact, the battery would run out quickly, and the end solution would be both bulky and cost prohibitive. As a result, the client decided on three main features: geofences and location tracking, issuing voice commands via a microphone-speaker combo, and a step counter.

Problem 3: Misunderstandings among team members

A business analyst helps get your team—production, IT, and business departments—on the same page.

Use Case:

Consider a factory that still uses outdated equipment. Factory workers might think their machines need to be equipped with temperature sensors to detect overheating and automatically turn off the equipment. The business department might suppose this is a waste of money. The IT department will be caught in the middle of the dilemma with different considerations—supporting the solution infrastructure.

Business analysts can help bridge the gap between various company stakeholders, consult the IT department on how to craft a solution that requires minimum maintenance effort, and present an analysis of cost savings that the business department can agree to.

Things to Remember

Business analysis in IoT projects is fundamental. When a skilled business analyst works through the project lifecycle, they help unlock the true potential of IoT, save on development costs, make business processes more efficient, train your employees on the new technology (if needed), help process client feedback, and implement corresponding changes.

The Future of the IoT Market

Although Verizon is looking to expand its 5G network to 60 US cities by the end of 2020, European and Asian telecom companies have put similar projects on hold. Without an efficient infrastructure, the future of IoT solutions that process large volumes of data closer to the edge of the network (surveillance cameras in smart cities, industrial robots, self-learning smart home devices, etc.) remains uncertain.

Industries react differently to the new pandemic reality. For example, the global logistics industry loses $350 million per week due to lockdowns, while smart speaker, wristwear, and personal audio device sales are projected to grow 9.8% in 2020.

Consumer IoT vendors will have to shift focus towards communication and entertainment technology to meet their revenue targets.

Which Economic Factors Are Shaping the IoT Market?

IT Spending is on the Decline

Before the quarantine, the business IoT market had been growing at a steady pace. The majority of companies had moved from IoT project planning to implementation and increased IoT investments by 20%.

Then the virus emerged, and the global economy slid into recession. Through 2020, businesses focused on restoring negative cash flows, optimizing the workforce, and adjusting capital expenditures.

As companies are pulling back on near-term infrastructure investments, hardware-related projects will see the sharpest cut. Software solutions, on the other hand, will display a modest 2% growth driven by the increasing demand for collaborative tools, document management software, and cloud solutions.

The pandemic crisis will lead to a 2.7-5% decrease in global IT spending.

Supply Chains in Chaos

Due to the quarantine and overreliance on China's manufacturing power, 75% of companies are reporting supply chain disruptions. It is estimated that the coronavirus outbreak has already caused a 12% decline in smartphone production, while smartwatch brands registered a decrease of about 16%.

This will force technology companies to adopt a multi-supplier, multi-location approach to hardware manufacturing and support small and medium-sized enterprises involved in the production of hardware components.

In the long term, businesses will consider moving production facilities away from China. Wistron Corporation, one of Apple's manufacturing partners, has already voiced plans to assemble iPhone components at a new plant in India, while Google is set to begin the production of smart home products in Thailand.

In IoT, the supply of chips, sensors, and development boards may take longer to ramp back up to normal than in other business areas.

Household Finances in Bad Shape

As a result of the pandemic, consumers have cut spending on clothing, beauty products, and consumer electronics (except for home entertainment devices).

The application downloads for major consumer IoT solutions can serve as an indicator of customers' diminishing interest in connected devices. Philips Hue application, for instance, has dropped 30 places on the US Lifestyle iOS Apps chart since February.

With the global economy in a recession, IoT companies are seeking ways to leverage their skills, infrastructure, and products to fight both the economic and public health problems associated with the pandemic.

According to Yahoo! Finance, 35% of Americans admit the lockdown has affected their current financial situation.

IoT Technologies Currently Trending Up

The Internet of Medical Things (IoMT)

Besides telemedicine and remote patient monitoring (RPM) systems, which saw a 50% increase in usage last month, healthcare providers and digital health startups turn to IoT and AI-based analytics solutions to manage the COVID-19 pandemic.

Researchers from California are feeding temperature, heartbeat, and overall physical activity data collected via wearable devices to machine learning algorithms to prevent the virus from spreading further in affected areas.

Use Case:

Specialists from the University of Massachusetts Amherst (UMass) have created a custom device based on a Raspberry Pi board and Intel Movidius 2 neural computing engine. The IoT gadget helps detect people with flu-like symptoms in a crowd by distinguishing coughing from other sounds.

Wearables can also help reduce the workload and increase the efficiency of hospital staff. For this, patients who do not show COVID-19 symptoms could measure vital signs at home using wearable devices and securely send the data to hospitals.

The Industrial Internet of Things (IIoT)

In 2019, automation was seen as a factory job killer. Today, manufacturers resort to Industrial IoT to monitor equipment and production facilities remotely and prevent unplanned downtime.

According to Mark Muro, Senior Fellow and Policy Director at the Brookings Institution, investments in automation are often made during times of crisis. To innovate on the cheap, the industrial sector will most likely retrofit legacy machinery with the help of smart sensors, connectivity technologies, and cloud-based analytics solutions.

Digital Twins

Digital twins are virtual copies of real-world objects: devices, factories, and even cities. To create a digital twin, developers process sensor data in the cloud and visualize it using dashboards or extended reality. The technology could potentially help businesses create resilient supply chains, design novel IoT products, and model manufacturing processes.

Use Case:

The University of Virginia's Biocomplexity Institute has designed an AI platform that simulates urban environments. The solution features virtual replicas of transport infrastructures and power grids and simulates the day-to-day activities of city dwellers. The research group is planning to combine the epidemiological data provided by the World Health Organization with the information they used to build the platform. This would allow US officials to predict the impact of lifting the current quarantine measures early and calibrate the virus response.

Another example comes from Unlearn.AI, a technology startup that created "digital twin" profiles of clinical trial patients and raised $12 million in its Series A round.

Drones

In 2020, new use cases for unmanned aerial vehicles (UAVs) have emerged. China successfully employs drones to transport medical samples, spray disinfectants in the streets, and detect citizens ignoring quarantine rules. Police departments across the USA are using surveillance drones to enforce social distancing in areas inaccessible to patrol cars. Farmers turn to drones and GPS technology to monitor crops and make better replanting decisions. But it's drone delivery that has made the biggest step forward. Zipline, a California-based drone delivery company, is helping the Republic of Ghana to assess the spread of COVID-19 by delivering test samples collected in rural areas to medical labs in the country's two largest cities. This marks the first time UAVs have been used for regular long-range deliveries in urban areas.

IoT Security Solutions

Recent studies show 57% of connected devices are open to medium and high-severity attacks, while 98% of all IoT traffic remains unencrypted. High-tech medical equipment turns out to be an easy target for cybercriminals, and 82% of hospitals that make use of IoT solutions have experienced at least one attack in the past 12 months.

As more people work from home and interact with healthcare providers via telemedicine solutions, IoT security (or lack thereof!) has become critical. To solve this problem, IoT vendors will use AI algorithms to continuously scan hospital IT infrastructures, force over-the-air firmware updates on devices with smaller hardware footprints, and make use of cloud-based security monitoring tools.

Things to Remember

The pandemic and the resulting lockdown have reshaped our economy and the way people control their finances. As household incomes are generally on the decline, consumer spending on connected devices is decreasing for the time being. Additionally, IoT vendors are suffering from disturbances in their supply chains.

Despite all the COVID-related difficulties, some IoT solutions are still trending as they help to battle the pandemic or make our life easier under the new restrictions. These solutions include the Internet of Medical Things, digital twins, drones, and the Industrial Internet of Things.

Conclusion

Despite forecasting a bright future for the global IoT market, managers continue to witness the repetitive failure of their IoT initiatives. This can be explained by the fact that IoT projects require a diverse skill set, significant investments, and are prone to security threats.

There is no IoT silver bullet, but you will be well prepared to face the challenges with the recommendations offered in this book. Finally, remember that failure doesn't always have technical roots. A company's culture and mindset can also play an important role.

Are you looking to start an IoT project and need help with ideation, vision, and scope?

Send us your initial project description

SEND