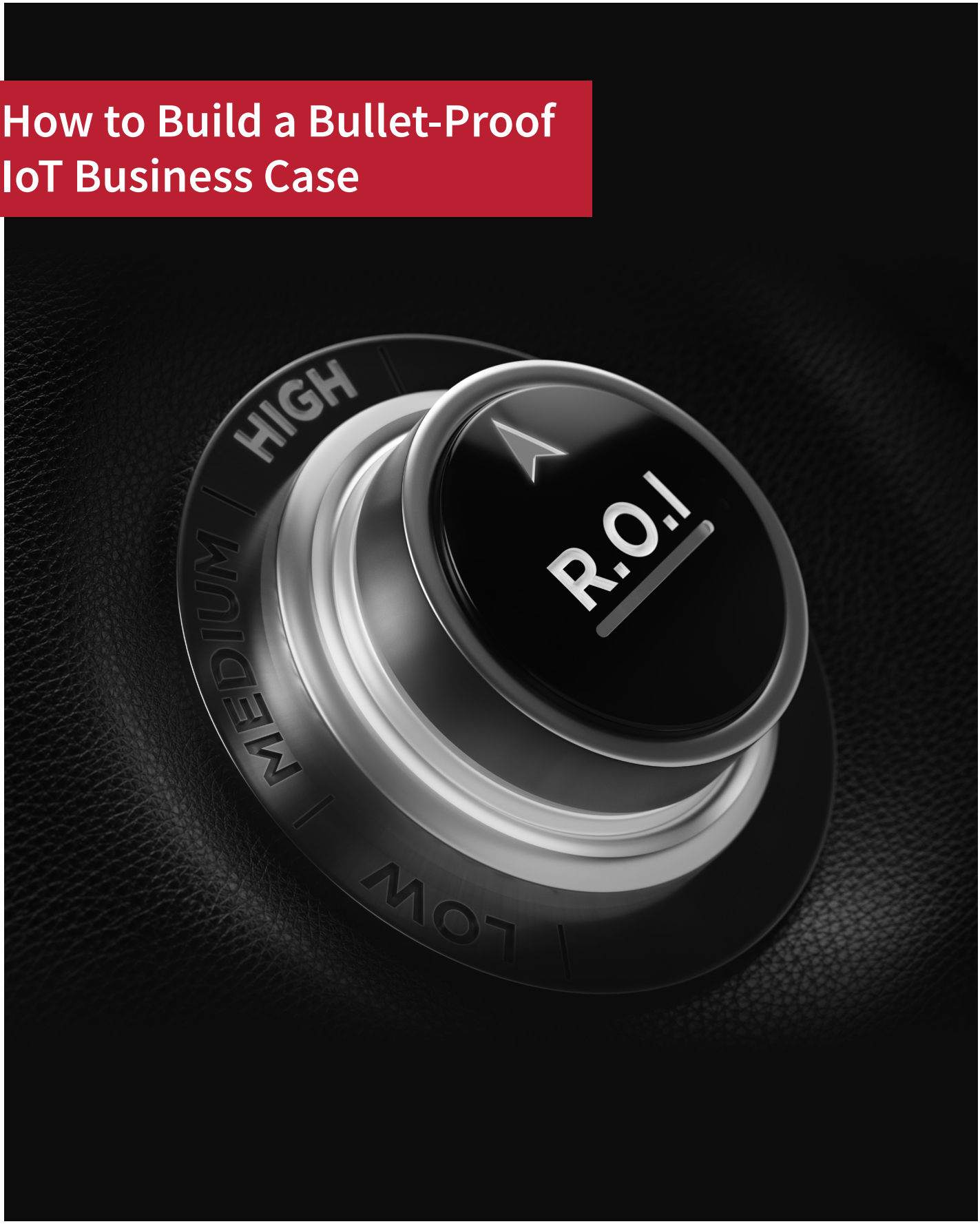
IndustryWeek

HOW TO ACHIEVE SUCCESS WITH THE IOT

Achieving success with the Internet of Things (IoT) requires a lot more than just selecting the right technology. This helpful guide tackles the aspects of IoT implementation that companies wrestle with the most, such as creating a strong business case, managing security requirements, and identifying the top requirements of a successful system. We also take a deep dive into the most common challenges that early IoT adopters have encountered—from budget constraints to cultural resistance to change—with advice on how to overcome these challenges to obtain real and tangible benefits.

How to Build a Bullet-Proof IoT Business Case



The IoT has the potential to lower costs, improve productivity, enhance safety and open new markets by changing how a company acquires, communicates, stores, analyzes and visualizes data. But despite what appears to be obvious benefits, building a bullet-proof IoT business case can actually prove to be quite elusive. However, it is not impossible.

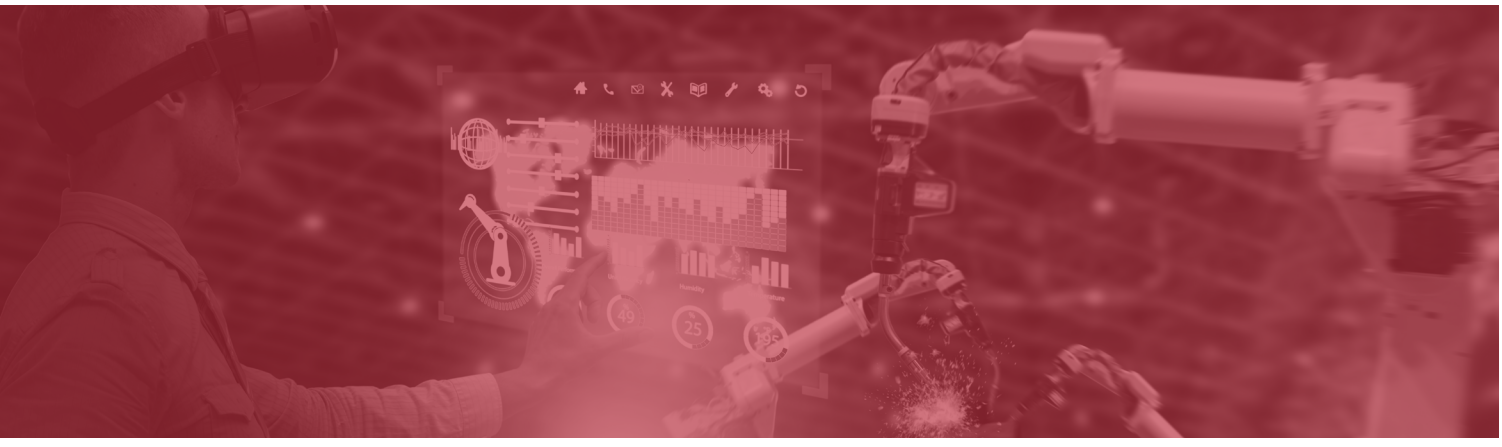
To create a solid business case for IoT projects, follow these general guidelines.

Think Business Problems

Focusing first on the technology and how it works is the number one mistake people make when building IoT business case. Sure, technology is cool. But the most important thing to include in the business case is a clear articulation of the business problem that the IoT implementation will solve. Will it lower operating costs? Improve production? Improve compliance? Open a new market? By describing the problem in business terms, the business case will help reinforce why an IoT project is important to the company.

Articulate Value

Not only should the business problem be defined, but the expected value to be realized should be stated in the IoT business case. An order-of-magnitude estimate is sufficient at this point. Keep in mind that no matter how great the solution, if the value realized is small, management will direct resources to other projects. The components of the expected value should also be included. For example, rather than quoting a lump sum, such as “maintenance costs will be



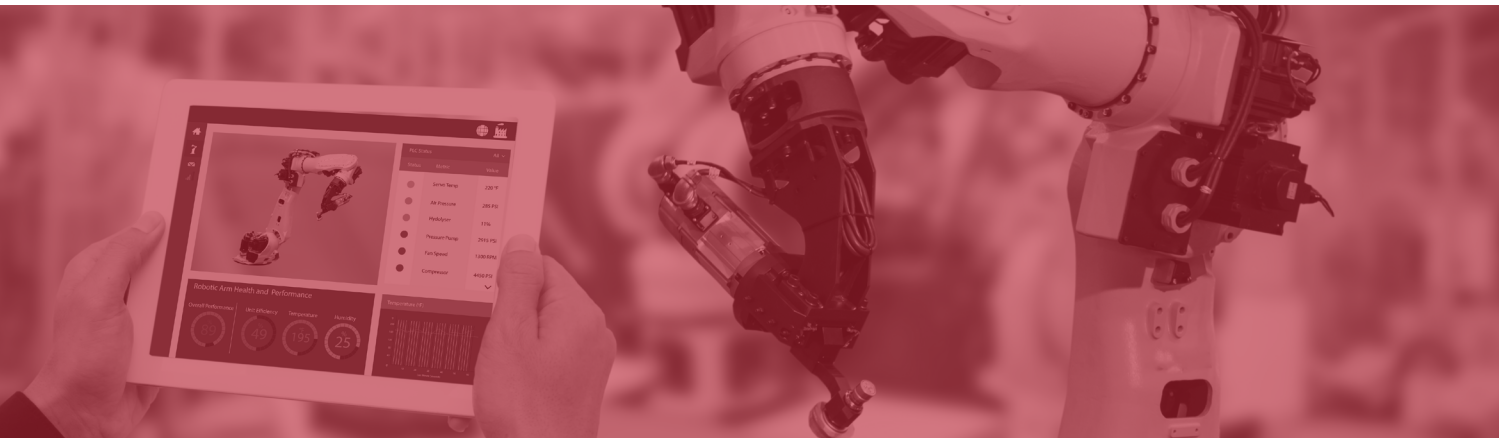
reduced by $100K," state the specific savings: 1) reduced transit time (-$10K); 2) elimination of unnecessary routine maintenance (-$45K), and 3) elimination of costs associated with unplanned outages (-$45K).

Know Your Customer

All too often IoT projects are considered to be infrastructure or IT projects. However, the true "customer" is the department that benefits from the specific business problem being addressed. The people in the customer organization—typically reliability engineers, maintenance supervisors, or plant managers—need to be convinced of the business case—not the technology people. A business case should be written to make sure the benefits to the true customer are clear and focus less on the technical details.

Change Behavior

The IoT is not about technology. The IoT is about using digital technology to change the way an organization conducts business to gain a competitive advantage. As a consequence, the business plan needs to show how the project will change behavior, business processes and workflows—without these advantages, the project will not create enough value. The business case should describe the change mechanism and what the new behavior will look like. Will there be less travel by personnel to service machines? Fewer manual readings? More informed decisions? The business plan must convince the intended audience that change can and will occur.



End-to-End Solution

One of the key concepts for generating value is to ensure that the IoT project generates an end-to-end solution. Below are five basic things that the project needs to generate value. Without all five, data will become "stranded" and the full value of the project will not be realized.

Sensors: All sensors required to take a machine's measurements.

Communications: Communications and protocol conversions to relay data from the sensors to the gateway to the enterprise.

Big Data Collection and Management: The ability to collect and store contextualized big data from virtually any source in order to identify patterns, detect trends, and build predictive models.

Analytics: A powerful analytics engine to make sense of the data so actionable insights can be found and employed in end-to-end solutions.

Visualization: Ability to display complex information and data sets in an easy-to-understand visual format for all users, regardless of skill set.

Explore New Business Models

One of the more exciting aspects of IoT is how it enables new business models, some of which are shown in the figure below. In a conventional implementation, the customer procures the hardware and various software components such as the operating system (OS), databases and compilers, installs the parts, and writes the application. You would then run all aspects of the operations, including

patching the OS, fixing hardware failures and updating core software components. If the system fails to deliver the desired business results, the customer absorbs all the risk and the hardware and software suppliers still get paid.

With the advent of the platform as a service (PaaS), service providers deliver the infrastructure and many of the software building blocks (hardware, OS, SQL, NoSQL, business intelligence, machine learning) to the customer. Some PaaS suppliers provide pre-built application components such as equipment health. Unlike the conventional approach, this is a shared risk model where the PaaS is accountable for the delivery of essential infrastructure and core software tools, while your organization still writes the applications upon the platform. If the supplier does deliver the services agreed upon, they do not get paid.

There are also business models where the customer buys data as a service (DaaS). In this case, the service provider installs the sensors, backhauls the data to its cloud, performs the analytics and then delivers the information back to the customer. In the case of no data, no payment is made to the suppliers. This model moves all the risk to the supplier and significantly accelerates project implementation.

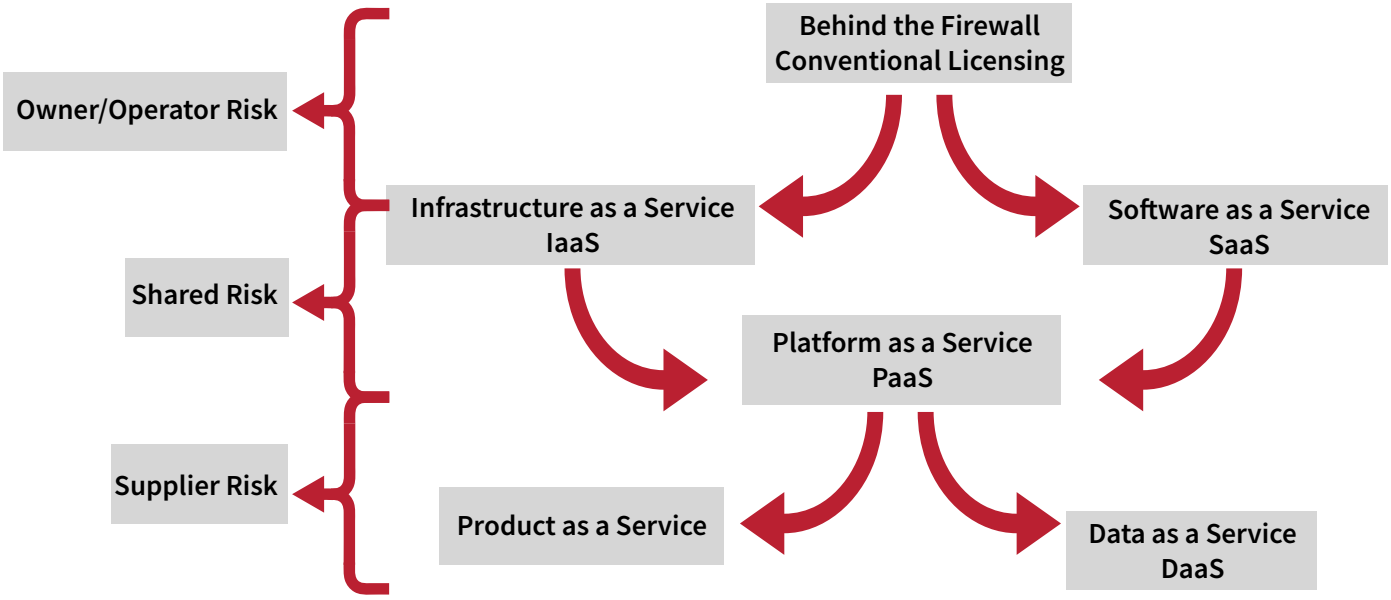


Figure 1 -In general, new business models that shift project risk in part or fully to the supplier result in lower CAPEX, faster time to market, and lower project delivery risk.

Move Beyond Proof of Concept

The business case must show how the solution will move beyond the proof of concept (PoC) and be implemented at scale. The greatest value is achieved when an organization achieves a step change in its basic business approach. Typically, small-scale implementations do not result in large step changes.

Most IoT projects do not pass the PoC stage due to the following reasons:

Cost and Complexity of Deployment at Scale: Setting up five devices in a lab environment is easy, but implementing 5,000 devices in the field can be hard. Make sure the solution is cost effective to deploy at scale and consider ways to manage those costs. One strategy might be to avoid costly, specialized skills in the field, opting instead for self-configuring devices.

Total Cost of Ownership: Be sure that the total cost of ownership is considered. For example, any time savings can rapidly evaporate when frequent trips to the field are needed to update devices and perform maintenance. In this case, consider whether updates should be pushed to all the devices from a central location.

Cyber Security: Many projects never move pass the PoC stage because the cyber security risk is too great, typically because security was an afterthought rather than an upfront consideration. Many of the "carpeted space" security solutions, such as user ids and passwords, do not scale in the IoT space.

Conclusion

IoT holds great promise to reduce costs, improve production, enhance safety and open new markets. However, it must be approached in a manner that generates a significant competitive advantage to the company. By following these guidelines, a solid business case for your IoT project can be created.

Early Adopters Weigh in on Unexpected Challenges of the IoT

In a recent survey by IndustryWeek, manufacturing professionals who had successfully launched an IoT project identified what they found most challenging, from the frustrations of dealing with their own slow-moving organizations to budget constraints.

When we set out to learn more about people's IoT experiences, the intent was to share the insights to help others embarking on their own IoT journey. Here's a look at those highs and lows—and steps you can take to plan for success.

First, the good news: Of the 270 professionals surveyed, the IoT project they completed either met or exceeded expectations for a reassuringly significant 86 percent.

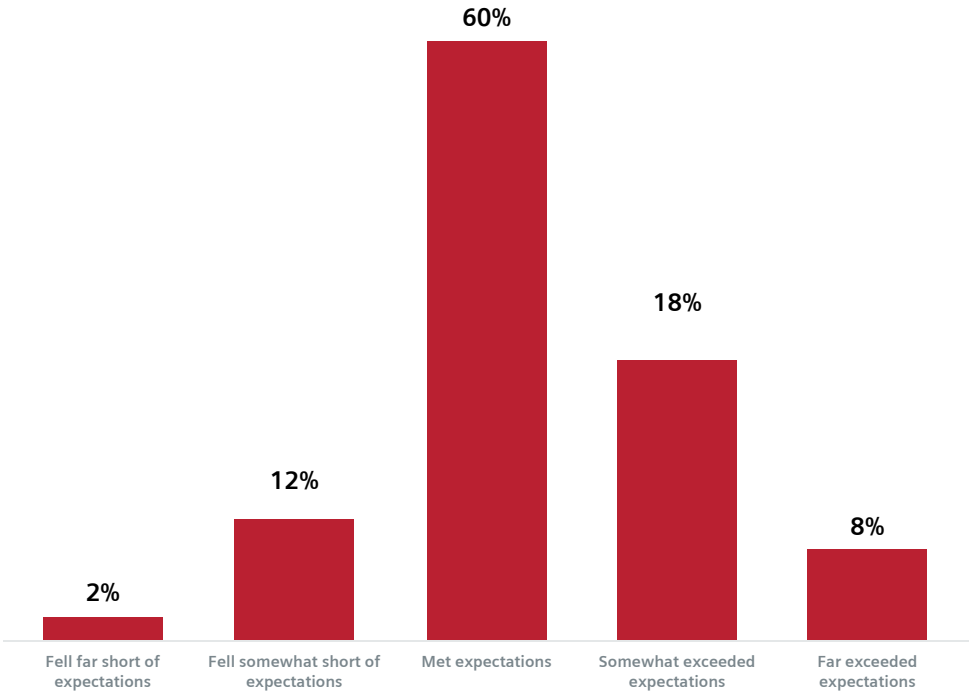


Figure 2 - Alignment of IoT Experience with Expectations

That's not to say success came easy, however, with only 17 percent of respondents claiming their IoT journey had been "not very or not at all challenging," while 84 percent found their experiences moderately to extremely challenging.

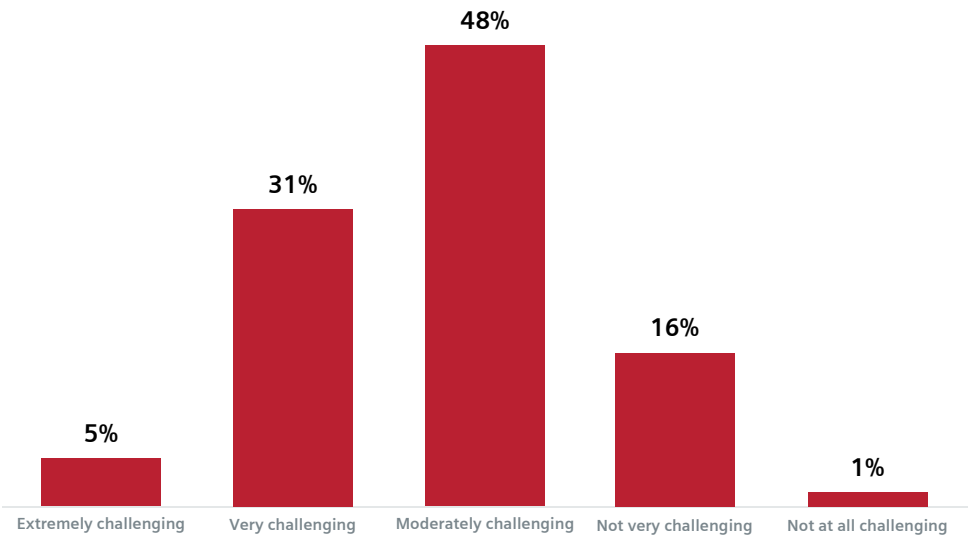
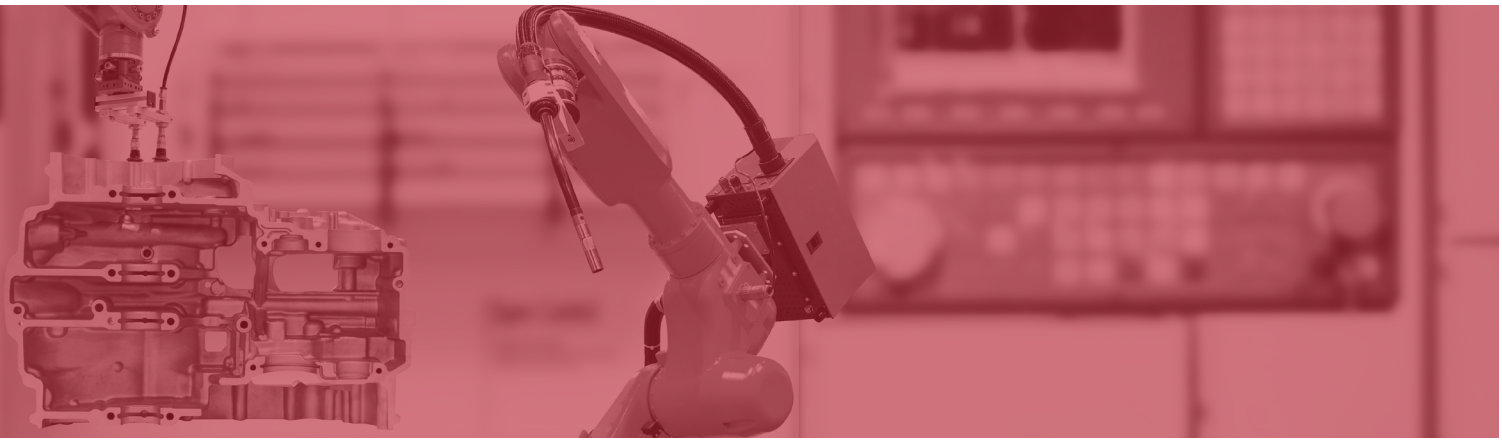


Figure 3 - How Challenging is the IoT Journey?

Clearly, every new technology comes with its growing pains and learning curves, of course, and IoT seems to be no exception. Broadly speaking, the challenges survey respondents faced in beginning their IoT journey can be broken down into a handful of areas:

- Steep learning curves
- Budget constraints
- Bandwidth issues
- Project delays
- Operational resistance to change

"Our IoT journey included a lot of new things that forced me to learn and change both myself and my team," noted one respondent. Others expressed



similar sentiments, describing the challenges of integrating new systems into existing equipment. Some discussed the cultural changes brought about by undertaking an IoT project, requiring new techniques and approaches to innovation.

With the abundance of new technology involved, some respondents felt that getting people up to speed and on the same page was cumbersome and time consuming at the start of the project, making things feel a little slow and frustrating. “It never works right off the bat like you think it will,” commented one respondent.

Others felt that the early days of an IoT launch involved a lot of “learning on the fly,” and that several iterations were required to figure out what actions would yield the best results or information. “We were constantly being introduced to new opportunities and issues,” noted one respondent, something that people also acknowledged comes with the territory with any new technology and should be incorporated into plans and project schedules.

For some, the learning curve was sufficiently steep that they were challenged by not knowing the right questions to ask or the various options available to them.

Constrained budgets and resources were another common theme, often going hand in hand with slow organizational adaptation to change, especially in large companies.

"Getting the buy-in to purchase software and hardware was challenging, especially as return on investment (ROI) is difficult to obtain and somewhat intangible," explained one respondent. Others noted that their company was simply not ready for the cost of equipment and upgrades, while others noted that justifying and maintaining resources had been difficult, forcing the projects to operate with extremely lean resources.

"It wasn't easy to determine priorities for the specific equipment or processes to migrate to IoT," added another, while some respondents also mentioned that their IT departments struggled with having the necessary skills to support the project and the resources to keep it going, with little to no help from other departments.

Schedule delays, too, had an impact on how respondents felt about the ease of implementing an IoT project. Some bemoaned the fact that things took rather longer than expected, with multiple test runs often required to get things set up and working optimally. Others noted it was the organization itself that slowed progress, because it wasn't yet equipped to handle the pace of change or the new IT infrastructure springing up everywhere.

"It turns out there are lots of 'moving parts' to complete each IoT project," explained one respondent. Another emphasized how important it is to think of it as plant-wide and not project by project.

Security also made the list of potential pain points, with some respondents expressing frustration over delays caused by concerns over data security and the need to ensure that data was correct and properly stored.

In short, the challenges of starting an IoT journey aren't that different from the difficulties encountered during the implementation of any new technology: There is often a steep learning curve, the need to prove the worth of the project to budget holders, shifting timelines, and endless scrapping for enough resources and support.

Overall, these "startup costs" of implementing an IoT project can be time- and budget-consuming without yielding obvious or impressive results early on. But the survey data suggests that once these obstacles are overcome, an overwhelming majority of teams are happy they pushed through and are now reaping the benefits. As one respondent put it:

"The nature of today's business is constant change, and as long as you have designed your IoT solution to adapt to change, you will be able to leverage it in order to achieve a real competitive advantage."

Despite some implementation challenges, respondents described the real and positive impacts, including the ability to gather information more efficiently, being able to monitor machine performance remotely, reduced costs in managing day-to-day operations, and the capability to get work done faster and better.

So, if you are about to embark on your own IoT implementation, here are some key takeaways from the professionals who have been there and done that:

- Don't create an overly optimistic timeline. There will be lots of new information to assimilate and things may not go according to plan.
- Be prepared to deal with ongoing budget and resource constraints and to scrap for every dollar until you demonstrate results.
- Be flexible and resilient; you'll need it to push through organizational resistance.
- Be prepared for skepticism from other teams and higher-ups until the project gains steam and/or yields results.

Top Five Requirements for Success with the Industrial IoT

There's no question that effective implementation of IoT in an industrial environment is extremely challenging. However, analysts following the rapid rise of IoT have almost universally agreed that the five requirements described in this article are essential for success.

Only a few years ago, few manufacturers had fully integrated industrial IoT into their equipment, but today there are hundreds. And although dozens of factors determine the outcome of industrial IoT-based asset management, analysts following the industry have found that nearly all successful deployments performed the following five activities.

These guidelines are written for project leads who have received approval to proceed with the financial resources needed to take the first few steps.

1

Create a well-rounded team.

Industrial IoT-based asset management is a project implemented on an enterprise-wide scale, which means projects should not only comprise IT staff. Team members should be selected from every part of the company affected by the project. Depending on how the company is structured, this includes managers from manufacturing, operations, service, product design and potentially others. Finding the best people has a lot in common with human resources (HR), so you might want to run your choices by HR before you approach a possible team member. And before you interview someone about joining the team, be prepared to explain in detail what will be required.

2

You will need help. Get it early.

Study after study has clearly shown that the most successful organizations rely on external specialists for their first industrial IoT project. That's because very few companies have all the knowledge required to implement industrial IoT-based asset management, including mechanical and electrical engineers, software developers, networking, security and certification specialists and people familiar with selecting and integrating communications protocols, sensors and other hardware.

A classic example of one task that will benefit from outside help is deciding which communication protocols to employ, how to connect legacy equipment and how to integrate them effectively. There are so many possibilities in this one scenario that without help from experts the process may slow to a crawl. It's also one of the reasons most often cited by companies that simply threw in the towel—after expending considerable time and money.

3

Establish your goals early.

According to several studies conducted since 2015, companies that considered their industrial IoT initiatives to be failures cited lack of focus as one of the main contributors. So, if you don't create a reasonable set of goals as a benchmark before you start, it will be impossible to judge what you've achieved. The goals must be reasonable because a project of this magnitude can easily promise more than it can deliver, as some of the first companies brave enough to wade into industrial IoT have found to their dismay.

This is a critical step, as it requires a thorough assessment of the scope of the project, identifying the metrics you want to improve and how to measure them. Understanding the key business metrics that are most important to you (that is, will produce a good outcome for the company) is essential—and difficult. Typical metrics include yield, throughput, uptime, efficiency and time to market. The good news is that even an incremental improvement in any one of these metrics can create outsized returns on investment.

4

Start small and scale up.

Armed with the knowledge you've gained in the first three steps, select a specific area within manufacturing that is small enough to implement quickly rather than attempting to modernize the entire organization at once. It should be an area in which success can be easily measured, which is often the one most in need of an industrial IoT-based solution.

For example, you can choose one key metric to improve and deploy a system capable of achieving it, using technologies such as edge computing and machine learning. During the process of putting this together, use the same technologies that will be scaled to serve more parts of the company in the future. Edge computing and analytics are relatively new to industrial IoT, so it makes sense to learn and implement them on a small scale and then scale up when the time is right.

5

Build in security now. Doing so later will be painful.

Cyber criminals will find a way to exploit vulnerable resources if they can gain financial or other benefits from the information. Early adopters of large-scale industrial IoT have already learned the importance of security because they have experienced intrusions. Early adopters didn't have or didn't know what resources to deploy to thwart cyberattacks. When an attack occurred, it meant that every port of entry, communications link, sensor, computer and other asset had to be explored as a security risk. This kind of reactive approach is expensive, time-consuming and embarrassing. It is imperative for success that security be built into an industrial IoT solution before deployment.

By making security a foundational element of your project—securing every port and device from the start—you will know what you have installed, how to maintain and upgrade it, and how to extend the system to other parts of the company over time.

Summary

Simply put, there are no shortcuts to a successful industrial IoT deployment. Successful deployments are strategic in nature, requiring the right mix of tools, processes and procedures.

Six Steps to Take When Implementing IoT Security

The gaping holes in corporate security are well documented and many companies are addressing them. However, most discussions about implementing IoT security merge it with enterprise security, which makes the process even more difficult than it needs to be. To help, the following six points describe the very first steps you should take to ensure security when starting any IoT implementation.

1

Establish a team dedicated to security.

The team should encompass representatives from global information security, IT, engineering, operations, and the vendor or vendors chosen to be the primary external supplier of resources and security expertise. Remember, these vendors will likely remain an essential part of your IoT team for a long time, so they need to fit and work well with your internal staff. That being said, be sure to conduct a security audit to determine if these companies or consultants meet your requirements now and have the resources to grow along with your company.

2

Produce an inventory of your industrial assets.

It's impossible to move forward with developing IoT security without first knowing what assets may or may not be affected. The effort required depends on how extensive the assets are and if multiple facilities are involved. Assessing each group and location individually is a good way to tackle this. The information you collect should include detail about all machines, including which ones can communicate locally or beyond and in what protocol, and other machines specific to each group or facility. This activity is vital to IoT security success because it provides the information required to perform all other activities in IoT deployment. Make it very comprehensive, regardless of how much time it requires.

3

Decide what equipment really needs to be connected.

Intelligence is moving toward the edge of the network. One of the benefits of edge computing is the potential to increase network performance by reducing latency. To minimize latency, a good rule to follow is that machines or other equipment that do not serve the company's interests by being connected to the Internet, shouldn't be. The results of an analysis based on this assumption will show that some will not serve the company's interests—even some that already have Internet access.

4

Identify the missing links and tap into people that have more extensive experience with security than you do.

Some of the ways that hackers can gain access to a device, machine, or computer are readily apparent, but others are not obvious. So, you should always complement your IT staff with cybersecuirty consultants who have years of experience and knowledge of current threats and scenarios, as things change frequently. Collectively, this team can identify all "ports of entry" and determine how to best seal them.

5

Learn about connecting legacy equipment.

Industrial equipment is built to withstand the rigors of the production environment for many years or even decades. So, it's likely that some of the equipment on your list has minimal connectivity capability or possibly none at all. Fortunately, as more companies implement IoT, solutions are available from various sources to help solve this problem. Typically, hardware is made "connectable" by adding wireless-enabled sensors and software, and these solutions almost invariably address security. The best approach depends on many factors, such as the age of the machine and the software that runs it,

and if it already has some ability to communicate. It's likely, though, that this equipment will need particular scrutiny as it's being brought online, as it will not have the latest security features.

6

Determine if some machines, computers, or other equipment should be replaced.

Although retrofitting existing (and typically expensive) hardware is comparatively simple and can be inexpensive, there are other factors to be considered as well. For example, if the financial resources are available, it often makes sense to replace legacy equipment. A new machine will invariably have at least one type of modern onboard connectivity as well the latest security features and will run on standardized software.

Summary

It's not surprising that large-scale IoT deployments are an increasingly appealing target for cybercrime. They have hundreds, even thousands, of possible points of entry (the attack surface), from wireless-enabled sensors at the edge through the IoT gateway and outward to the cloud. Only by scrupulous attention to every one of these points can security be reasonably assured, and this requires more than the minimal password maintenance, firewalls, and other fundamental tools.

The process is hampered by many factors, most notably by the fact that IoT itself is new and there is no single standard or overarching set of standards that define it. In addition, many of IoT's constituent parts were not designed to be inherently secure, might not have the memory or other resources to implement security, and may operate on numerous incompatible protocols. That said, of all the elements in an IoT deployment, security will prove to be the most important in the long term. The time and money required to implement and maintain it will be well spent.

This content was developed in partnership with Siemens Digital Industries Software.