Making Everything Easier!™

Special Edition

The Internet of Things For Dummies®

A Wiley Brand

Compliments of

CGI

John Hicklin
Bill Shurvinton
Gemma Beard

About CGI

Founded in 1976, CGI is a global IT and business process services provider with 68,000 professionals in 40 countries across the Americas, Europe and the Asia Pacific. CGI delivers high-quality business consulting, systems integration and managed services that drive the ongoing evolution of their clients' businesses.

Across the UK, CGI has around 6,000 members with specific industry knowledge and a broad range of client experience, making CGI a true local partner.

CGI has a long track record in connected devices, both in the UK and internationally, and brings this wealth of knowledge and experience to its clients through the CGI IoT solutions team.

CGI's award-winning IoT solutions cover a wide range of industry sectors—from transport and utilities, to the public sector and defence and to engineering and smart buildings. CGI has at the forefront of delivering predictive maintenance to a global elevator company, traffic and transport management solutions to cities and public transport providers, and journey and virtual travel planning services to enhance the travel experience of commuters and passengers. CGI provides smart road lighting systems, saving money and making road travel safer, as well as electric vehicle charging and in-car communications technologies that transform the way we drive. CGI has the sector experience, credentials and track record to help clients realise their IoT visions.

CGI

Experience the commitment®

www.cgi-group.co.uk/solutions/internet-of-things
IoT.uk@cgi.com

f facebook.com/CGI.UK
twitter.com/CGI_UKNEWS
in linkedin.com/company/cgi
You Tube youtube.com/user/CGIGroup

Internet of Things FOR DUMMIES

A Wiley Brand

CGI Edition

By John Hicklin, Bill Shurvinton, and Gemma Beard

FOR DUMMIES
A Wiley Brand

Internet of Things For Dummies®, CGI Edition

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom *For Dummies* book for your business or organisation, contact CorporateDevelopment@wiley.com. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER, THE AUTHOR, AND ANYONE ELSE INVOLVED IN PREPARING THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-1-119-04330-0 (pbk); 9781-1-190-4337-9 (ebk)

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

CGI acknowledgements: Special thanks to Paul Hopkins of CGI's Cyber Security team, Ian Glover of CGI's UK Marketing team, and Danny Wootton of the CGI IoT team. CGI would also like to thank Steve Dunbar from Microsoft and Andrew Orrock from Arkessa for their contribution to this book.

Table of Contents

Introduction

The Internet of Things (IoT) is the latest technology trend capturing business and consumer attention. You only have to scan the press, analyst reports and social media to realise the huge potential for IoT.

The numbers of "things" that many analysts think will be connected by 2020 keeps expanding. Currently, they anticipate that there will be many more connected devices than people; estimates range from 24 billion to over 200 billion connected devices delivering economic benefits valued between $2 and $9 trillion!

About This Book

But is the hype surrounding IoT justified? Already, people are raising many questions:

- What does the term IoT mean, given that it's being applied to such a diverse range of applications?
- In what ways can this technology wave bring real benefits to businesses and consumers?
- With all this new connectivity, how secure is personal or corporate data going to be?

This book addresses these and many more questions. Those of you familiar with previous CGI *For Dummies* books know what to expect: a concise guide that brings you up to speed with IoT. This book also provides background, context and definitions that cut through the jargon, as well as impacts and issues that you may come across as you embark or continue on your IoT journey.

Foolish Assumptions

In writing this book, we make some assumptions about you (forgive our presumption!):

- You work in a business role within your organisation and have a basic understanding of the technology trends that face your sector.
- You want to know more about IoT—what it can do for you and how it's likely to benefit your company or organisation.
- You have an interest in how business functions can work better together, and this helicopter view can help you to see how IoT impacts operations as a whole.

How This Book Is Organised

We divide this book into the following chapters:

- **Chapter 1: Connecting to the Internet of Things Revolution:** Get to grips with the essential definitions and the technology enablers.
- **Chapter 2: Appreciating the Impact of IoT:** Understand how IoT can impact all parts of society.
- **Chapter 3: Beginning Your IoT Project:** Design an effective project and stroll through some IoT examples.
- **Chapter 4: Getting under the Skin of IoT:** Get the lowdown on what makes up an IoT solution.
- **Chapter 5: Delivering Your IoT Solution:** Work through your approach to implementation.
- **Chapter 6: Securing Your IoT:** Be aware of the threats that you face, and know how to combat them.
- **Chapter 7: Ten Handy Hints for IoT Success:** Set out on the right foot and help your project to run to plan.

Icons Used in This Book

To help you find particular pieces of information as easily as possible, we use the following icons to highlight key text.

TIP This icon points to helpful hints about IoT.

REMEMBER Take note of text beside this icon because it highlights important information to bear in mind.

WARNING! This icon indicates practices and situations to be aware of. You'll be glad you did!

REAL WORLD We include a number of real-life examples to illustrate important points.

Where to Go from Here

As with all *For Dummies* books, you can read this one however you like. You can dip in and out or read it from cover to cover. Despite being packed with useful information, it won't take you long, and it may save you a lot of hassle!

Use the headings and cross references to guide you to the information you need. If you require any more information, feel free to contact us at `iot.uk@cgi.com`.

Chapter 1

Connecting to the Internet of Things Revolution

In This Chapter

- Defining Internet of Things
- Identifying the technology changes behind IoT
- Climbing aboard the IoT train

No one likes to be left out of things, especially when it comes to the Internet and communication technology where so many new products and services are emerging.

People use the phrase *Internet of Things* (IoT) to describe a number of different technology developments, including advances in the design and manufacture of chips, new communication services and gateways, cloud computing and so on. This varying usage makes the area quite confusing and tends to obscure the key value that these impressive new technologies can unlock.

Understanding how the connectivity of *things* came about helps you cut through this confusion, which is one of our aims in this book.

REMEMBER

For clarity, a *thing* in this context can be any source of data, machine or wearable technology — for example, an electricity meter, an aircraft or an armband monitoring your heart rate. All these items can be made to communicate and become "smart". But the level of deployment or sophistication of such solutions varies, and so seeing how IoT technologies can help to advance these services or create new ones is the key to appreciating its potential.

In this chapter, we introduce you to IoT — what it is and how it can help your business or organisation.

Differentiating Internet of Things from M2M

Kevin Ashton from MIT is credited with coming up with the term *Internet of Things* (in 1999) in regards to work undertaken there to understand the potential of low-cost sensors on daily living and the home.

But of course the idea of connecting devices is not new, and you may be wondering whether IoT is simply another name for describing existing M2M solutions (which we briefly describe in the nearby sidebar "Moving from M2M to IoT") or whether a more fundamental concept underpins the use of this different term. Well, read on for the answer. . .

Moving from M2M to IoT

Prior to the use of the IoT label, solutions involving connected things or devices were referred to as Machine to Machine (M2M), SCADA (Supervisory Control and Data Acquisition) or telemetry. People often use the term M2M as a generic term for all such systems, but here we describe the other two briefly for background information:

- **SCADA solutions:** Typically deployed for manufacturing, transport or utilities (for example, Network Infrastructure Monitoring and Control), these solutions combine monitoring and remote control capability, such as production line control or electricity distribution networks.
- **Telemetry:** This term is typically restricted to simple monitoring — for example, the monitoring of power usage or pumps in an industrial context. The term was also used for tracking vehicles, such as with public transport. Such solutions were dedicated to particular purposes and generally isolated from the other IT and service functions within the user organisation, with the information locked into specific operational silos.

Clarifying the difference between IoT and M2M

Many different definitions seek to draw a distinction between IoT and M2M. At CGI, we go with the following:

- **IoT:** A world where smart objects are seamlessly integrated as part of a global network; where smart objects interact without human intervention to deliver new services or improved processes beyond the silos and across the business. IoT redefines the way humans and machines interface and how they interact with the world around them.
- **M2M:** An enabling technology that delivers the communications component of IoT to clients. In general, communication providers such as telcos provision this technology.

Locating IoT's true potential

Drawing out the distinction between IoT and M2M helps to clarify where the potential for IoT lies:

- Although IoT has tended to have a device- and consumer-orientated focus, the capabilities it offers are directly applicable to any organisation or enterprise and have the potential to drive operational efficiency and the launch of new consumer services.

  This fact is significant because the value of IoT is going to be recognised within the business market. This business value will drive consumer benefits such as new services and enhanced life experience, which was the original vision for IoT.
- The use of IoT in organisations enables services to be delivered where the data acquired from things or assets can be used across the business, not just restricted to specific business functions and users (as with M2M solutions). As such, IoT can offer a potential complement to existing services, which need to be maintained for operational reasons, or a replacement where their cost has

become prohibitive for continued use. The opportunity also exists for organisations to deliver new services that haven't been deployable until now for technical or commercial reasons.

Such IoT solutions can also share core application functions — for example, a security framework, message handling or data processing. This helps in increasing speed of deployment and reducing costs of ownership. This approach means lower-value assets or things, not previously viable for inclusion in costly M2M solutions, now have the potential to be smart. For example, individual items in a container (not just the container itself) can be tracked, and bearings in an escalator (not just the escalator itself) can be monitored, as can fire alarm sensors and not just fire detectors.

- The value from adopting IoT is the exploitation of the near real-time data generated, helping employees and customers to be better informed, to make decisions and to improve their life or work experience. We call such information *actionable insights* (we refer to this phrase throughout the book). In contrast, real-time SCADA systems in manufacturing (for example, in robotics) restrict the use of the data to the factory environment, and M2M solutions have been focused on connectivity and collecting data, with some organisations having more data than they know what to do with! IoT goes beyond this by enabling data to be transformed into information that improves productivity, decision-making and the customer experience for the whole organisation.

Looking at the Technical Drivers for Change

IoT is made possible by the grouping together of a number of technological developments, including scalable computing power, sensor capability, cost and size reductions, the varieties and costs of communication and, in more recent times, advances in data analytic tools (see Figure 1-1).

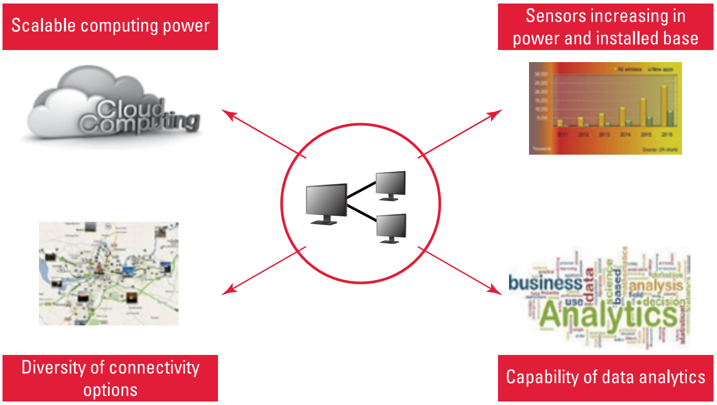
Scalable computing power
Cloud Computing
Sensors increasing in power and installed base
Diversity of connectivity options
business
data
analysis
Analytics
Capability of data analytics

Figure 1-1: Technology enablers for IoT.

In addition, more people are embracing IoT because many of the challenges for M2M adoption have been overcome. We discuss those challenges in this section:

- Initially, the purchase and installation of a device and the necessary bespoke software development to enable communication for an M2M solution were costly. As a result, the monitoring of an asset was only operationally viable for high-value assets (for example, remote points control in the rail industry).

  Over time, however, sensor and device functionality increased, but the costs fell, and so smaller assets (for example, white label domestic goods, ball bearings, items of clothing) can now have connectivity and be monitored.

- The broadening array of short-range wireless services and the drop in costs for fixed and mobile-wide area connectivity also contributed to a growing range of potential scenarios for connectivity and hence monitoring and control.

  In-building coverage and the ability to connect sparsely populated geographies is now possible with, for example, hybrid communication solutions.

- Cloud computing improves the speed of deployment and the cost of developing and maintaining applications. The sharing of infrastructure and indeed application functions such as workflows and analytics impacts the IT commercials, further extending the potential for new usage scenarios. It also offers the potential for the inclusion of further data sources and application integrations to add value to existing solutions and create new innovative services and access to new data-analytic capabilities.

Becoming Part of the Emerging Market

Some of the confusion surrounding IoT arises because multiple technologies are converging around a single service. Device manufacturers, software providers, mobile networks and others all have a part to play and therefore see the IoT offering from their particular technology viewpoint.

REMEMBER

It's important to be focused on the business transformation that is enabled or unlocked. We view the opportunity as having the potential to gain operational efficiency while also providing innovative customer experiences from a single technology investment.

Recognising the benefits of IoT

Knowing where to start can be a challenge given the vast array of connectable things or assets. But clearly, you need to maintain a focus on key areas of potential value. We highlight some general areas in the earlier section "Locating IoT's true potential" but get more specific here with some types of IoT solutions:

- **Enable prediction of health and performance of things and people:**
  - Relevant to any process involving the management and support of equipment, such as lifts, boilers, fridges and air-conditioning, where the key objective is to keep the equipment running at optimal efficiency.
  - Equally relevant to maintaining the health of a person, with applications emerging in the consumer market that feature wearable technology and that monitor patients in their homes.

  - Applicable to maintaining the skill level of a maintenance engineer by providing prompts for faults they are working on while on-site.
  - Also possible to optimise processes by remote control of assets.

- **Mobile and fixed asset management:**
  - Relevant to scenarios where fixed and moving assets exist and the requirement is to manage both assets together to achieve a business mission. Impact can be seen in the supply chain, vehicle tracking and maintenance.
- **Data brokerage and finding value from data:**
  - Focuses on delivering new and insightful data that's valuable to the client's internal business processes, customers and/or suppliers. The ideal scenario is one where data can be sold as part of a new service or is used to support the enhancement of a current service to differentiate the client from the competition.

Check out Chapter 2 for more areas that IoT is sure to impact.

Making IoT work for you

Looking at areas where you're already collecting data is certainly worthwhile. But also recognise that more can be done to extend such solutions in, for example, the area of customer management, operational support or business planning where you can derive further insights. Taking advantage of cloud services enables you to evaluate pilots and innovations technically and commercially without major outlays of investment, improving your chances of picking the most likely to succeed. This opportunity is in stark contrast with the past.

Deploying IoT solutions involves drawing together partners with specialist knowledge and experience to bring services to market. The key to success is to focus on immediate business benefits and to offer truly enterprise-ready, proven approaches with recognised technology providers.

Enterprises investing in and realising the benefits of the technology are going to drive IoT, instead of simply consumer demand. Opportunities clearly exist for original equipment manufacturers (OEMs), and they're already seeing the potential for new devices and communication to support IoT services in the enterprise.

As these solutions develop, enabling low-cost monitoring of environmental, operational or service events, the enterprise benefits and becomes able to access increased gains.

If you're still unconvinced, turn to Chapter 3 for a couple of case studies that provide compelling evidence. If security is a concern, flip to Chapter 6. But if you're ready to begin with your own IoT, Chapters 4 and 5 contain all you need to know for getting stuck in.

Chapter 2

Appreciating the Impact of IoT

In This Chapter

- Discovering the potential effects of IoT
- Improving the structure of society
- Impacting society from top to bottom

Too often people and businesses are content just to jog along comfortably, unchallenged by new innovations and possibilities. At least they are until, one day, they realise that rival firms have left them languishing far behind.

Technologies such as cloud-based analytics, sensor deployment and power and connectivity options are making the exploitation of near real-time data a commercial reality. The enhancements to information management that this data makes possible can deliver business value for enterprises in many ways: Manufacturers of consumer goods can engage with their end users in new ways and facility management can be transformed across sectors through integrated remote management of properties, impacting maintenance, energy consumption and leasing models.

In legacy M2M applications, business benefits were closely aligned with specific users, usually monitoring high-value assets/operations. But in the new world of IoT, staff across an organisation can benefit from the insights derived from monitored assets. These insights increase their productivity and operational awareness. Businesses can also benefit from solutions developed for other sectors, given the common underlying technology. It's also possible for organisations to broaden the range of monitored devices, giving increased insight and the potential to launch new services.

In this chapter, we take a look at what this always-connected, always-on world offers to government, businesses and consumers in the short and long terms. Be in no doubt that the developments are going to have a cumulative impact across society as a whole.

Feeling the Power of IoT

The immense significance of IoT is that it brings together all sorts of technology developments in order to enable actionable insights (which we explain in Chapter 1) from the data generated by things, and to transform how people interact with machines and how machines can interact with each other.

REMEMBER

These actionable insights will enable a fundamental change in how business and society operate:

- **Proactive and preventative:** A change from health to asset maintenance will cause a fundamental shift as people look proactively for the causes of issues (insights) and take early-stage action in order to prevent, where possible, a larger issue.
- **Data-driven business models:** Businesses will migrate from a subscription or "flat fee" based model to ones based on usage, time, duration, load, risk and so on, fundamentally changing how people buy and consume products and services.
- **Interconnectivity and collaboration:** A move from "siloed" datasets to an interconnected world in which trusted parties subscribe to published data will shift businesses to a position where they learn from other people and organisations in order to enhance their own performance.

Transforming Society's Infrastructure

Don't underestimate the huge potential changes that IoT can bring to the world around you. As we describe in this section, the innovations range from transport and construction to personal health and homes.

Travelling into transport of the future

The longer-term vision is that IoT will deliver a step change in quality and capacity in transport systems across an entire city region. It will do so by, where appropriate, consolidating and integrating local authority operational transport management functions, both public transport and highways, into a single critical hub.

REMEMBER

Interconnectivity will provide a single holistic approach to transport management with close coordination across all modes, including walking, cycling, electric vehicles and car-share schemes. It will also enable logistics operators to proactively adjust the provided capacity as well as the routes and services offered to the public and business.

In the short to medium term, the smart city of the future will be able to leverage existing system capabilities (for example, active traffic management) and live data feeds from multiple sources (such as live vehicle flows, ticketing systems and crowd flow monitoring) to improve processes, workflow management and decision-support capabilities. Looking farther ahead, IoT will provide a fit-for-purpose, "joined-up" approach to managing transport, scalable to meet current and future demands associated with economic growth objectives as well as the social needs of a changing demographic.

These joined-up capabilities will enable city regions to be better placed to balance the true needs of public transport with those of private/commercial motorists, acting as a major catalyst in the creation of a new model for sustainable economic growth and delivering a much more connected, more talented and greener city region. An added benefit is that cities will be able to achieve cost efficiencies through the removal of role duplication while at the same time significantly improving communications between individuals and teams.

In the future, and when legislation allows, autonomous vehicles (or indeed aircraft!) will begin to impact the transport experience as camera and radar technology and machine-learning capabilities advance. These advances will further optimise the usage and sharing of transport networks, specifically in cities, and continue the trend towards merging private and public transportation into Mobility as a Service.

REMEMBER

One of the bigger challenges, and therefore addressable in the longer term, will be joined-up transport in rural areas, where for many people public transport is essential but sparse, and for others, it's currently not a viable option. The future will see coordination between public and private transport services and the public, as car sharing and public transport pick-ups are coordinated to allow people living in rural areas to benefit from a more frequent and more distributed transport network.

Enhancing future healthcare systems

The field of healthcare has a long history of connecting machines to machines. Since the 1960s, laboratory analysers have been connected to information management systems, and, since the 1980s, digital radiology machines have been sending complex images to rendering systems. These developments leave users on the cusp of a new way of connecting machines.

As devices and machines become more sophisticated, they expose more data and services via standard interfaces. The richness of these datasets and associated services now enables users to orchestrate complex clinical and organisational processes across multiple platforms to improve patient safety, reduce cost and improve the health of populations. All of these outcomes represent the Institute of Health Improvement's (IHI) Triple Aim objectives of

- Improving the patient experience of care (including quality and satisfaction)
- Improving the health of populations
- Reducing the per-capita cost of healthcare

Such orchestrations could see the integration of data and services to ensure patients needing transportation for an MRI — but who have a hospital-acquired infection — are not transported via elevators in which surgical patients are moved from the operating room to their rooms. Another example concerns using the numerous patient devices in intensive care units (ICUs) to ensure that people comply with best practices during high-acuity episodes. Merely connecting devices isn't enough; interpreting the data and orchestrating processes is where lives are saved and costs are reduced.

The potential for *tele-health* (which involves monitoring an individual's health remotely) is highly significant. Patients' use of small electronic devices often referred to as *wearable technology*, such as wristbands and smart watches, will enable continuous, accurate collection of data. Physicians can use this data, subject to an individual's agreement, for patient management and care, symptom management, medical research, clinical trials, treatment monitoring (tracking pills and so on) and predictive health monitoring.

In the long term, this technology will contribute to improved drug development and the efficiency of health-service delivery. The reduction in unnecessary journeys will have a positive effect on transport in cities, where health-related traffic is a significant contributor impacting the environment and productivity. The data collected can also be a source of information or insight that can be monitised, where appropriate.

The short term will see significant benefits to the health sector as people start to use IoT to monitor their own health and activity, independently of health professionals but in collaboration with social groups. This monitoring and interaction will rapidly improve the health of a large percentage of the population as individuals compare their own data with that of a similar demographic group, and through preventative health monitoring start to reduce demand on the health service.

The smart hospital of the future will be able to optimise the use of equipment for patient care by monitoring its location as well as ensuring that it's in working order. Bed use, energy management and the coordination of operations, bringing together the right resources, people and equipment, can all be significantly enhanced with the consequential improvement of patient care and operational cost savings.

Changing legislation will also cause changes in the insurance industry associated with the monitoring of individuals' health. The enhanced understanding of individual risk derived from monitoring health will lead to more sophisticated models for defining premiums. Additionally, the use of in-vehicle telematics devices is changing the way premiums are devised. It is not inconceivable that health insurance could go down a similar path. There are losers and winners in such developments, but it does enable personalisation of premiums that more accurately reflect the health risk profile for an individual.

Improving the industrial, utilities and manufacturing sectors

As early adopters of M2M, these areas will be able to exploit IoT technologies to bridge the "silos" between telemetry and SCADA systems (which we define in Chapter 1). The integration of data from these different systems will improve insights into process flows, whether through a manufacturing facility or a utility network of any kind, gaining improved control over the end-to-end process.

REMEMBER

IoT also creates the opportunity for new consumer services through data-driven business models. IoT-enabled finished goods can provide key insights into their performance to the original equipment manufacturer as well provide direct contact with end users, enabling the change from individuals buying a product to buying a service based upon usage and so on.

In the short term, smart meters in the home will provide energy suppliers with significant insights to enable proactive demand management by offering consumers such things as demand-based tariffs. In the longer term, we'll see the convergence of "as a service" and demand-based pricing because information from connected devices and the power usage stage can be analysed together.

TIP

Such information can also be a source of new revenue streams because such data can be of value to third parties who can use near real-time data for their own designs and operational planning.

For supply chains, the reduction in the cost of sensors makes the tracking of individual items, rather than pallets, realistic. Perhaps a firm can use the information from such items to optimise delivery and even extend it to trigger payments, instead of waiting for paper systems to be completed. In the longer term, end-to-end coordination of supply chains will become the norm, with stock management and warehouse systems coordinating with logistics and manufacturing companies to add further sophistication to "just in time" stock management.

Building and automating homes

Building management is an important issue across multiple sectors. Currently, a number of disconnected systems perform it, but IoT will enable a single view of building operation, allowing operators to visualise how one system or event is impacting others. The result will be improvements in energy consumption, maintenance schedules and how retail properties are offered for lease based on footfall.

TIP

IoT technologies can also monitor installed equipment ranging from fridges on the shop floor to vending machines. Combined with the building insight, it can give property owners and managers the ability to optimise the use of the facility and improve the customer experience by ensuring machines are located appropriately and are in working order. In the future, IoT will also enable building owners to maximise the use of their building throughout the day, enabling access and billing to companies in the daytime and to social groups in the evenings.

Changing Civil Society across the Board

Everybody lives in communities and groups, so the IoT revolution in communication is sure to leave very few areas of society untouched.

Looking at changing government and legal priorities

The connected future will impact policy making in a number of areas:

REMEMBER

- **Privacy:** The debate around data privacy for consumers, commercial organisations and government is already in the public domain, and this focus will only intensify. Bringing forward legislation that meets public-security and public-scrutiny requirements as well as individual rights will be required. However, the basis for such legislation can be seen in the "physical" world with defined property rights and agreed legal access by warrants supported across international borders and by inter-governmental structures.
- **Communication access:** As the range of communication services broadens and people's rights of access to information are enforced, the reliance on these services will rise above a luxury or convenience to a right that needs to be universal. Communications will therefore have to be legislated for in much the same way as utilities are today to protect the rights of the more vulnerable in society. This issue will also put a greater focus on maintaining such services and consideration around the need for the definition of what constitutes critical national infrastructure.
- **Legal issues:** As many of the IoT-enabled autonomous technologies come to market, legislation will need to be modified. Notions of ownership and exchange will be broadened, with the monetisation of data and transfer of goods and services undertaken by means of the new intelligent systems.

  For example, today an individual is insured and has a licence to drive a specific car. In the future, legislation

> will need to accommodate cars driving themselves and people driving a car that has been made available to them as part of a collaborative transport system.
>
> The drive for standards in device-to-device solutions will also enforce the need for compliance regulation, especially as solutions move into business-critical or safety-related services. There are also issues around security (we tackle these in depth in Chapter 6).

Considering the economic impact

IoT has the potential to drive not only operational efficiency but also new consumer services and ultimately business transformation. Such innovation will drive down production costs and enable industry and governments to benefit from digital transformation.

TIP

As this kind of adoption develops, IoT will add to the drive provided by smartphones and other devices for value creation in sectors supplying the technologies for deployment — for example, chip, sensor and device designers and manufacturers, as well as IT vendors and integrators.

Impacting social interaction

The uptake of smartphones and other gadgets has raised the public's expectations of connectivity. As IoT brings things into this consideration, it will create new experiences around sharing (defined by access rights) and even ownership (cars). For example, services like Zipcar and car2go are offering pay-per-use access to cars as an alternative to city dwellers buying and maintaining their own vehicles, and Liquid Space provides access to shared office and community spaces.

IoT will also enable far greater levels of social collaboration, particularly in health. A local community may have access to data associated with the elderly in their locality to monitor and care for those individuals, further reducing the burden on health services. For more impacts on healthcare, check out the earlier section "Enhancing future healthcare systems."

Challenging technology

The need for increased connectivity at low cost will drive chip- and device-based innovation, impacting the deployment of new wireless-based services. Much like setting up a smartphone, tablet or laptop has become common knowledge amongst the population, installation of sensors will, in the future, not require specialist skills. In many cases, sensors will be already built into everyday items or will be available in “blister packs” from local electronics stores.

WARNING!

At the same time, the exponential growth in information flow will place huge demands on communication networks in terms of capacity, coverage and speed, as everyone becomes accustomed to immediate access to their data.

It will also add to the momentum of cloud computing, with the increase in computing and data storage required and analytic services where organisations derive new value and insights to improve their efficiency and competitiveness. As a result, “data scientist” will become a familiar job title!

Investigating the environmental impact

Across all environmental scenarios IoT will have positive outcomes for carbon usage through energy management, reduced travel needs (see “Travelling into transport of the future” earlier in this chapter) and optimised supply chains.

IoT can also improve the monitoring of assets holding contaminants and chemicals, detecting when they are in a critical state or monitoring them in transit and ensuring they are dealt with appropriately. Improved insight means improved prioritisation of response in emergency situations.

Environment agencies can monitor the detection and assessment of natural disasters, such as flooding and landslips, more effectively in rural areas and manage them in a cost-effective manner.

TIP

As with improved healthcare (flip to the earlier section “Enhancing future healthcare systems”), these environmental areas will also have positive implications for the insurance industry.

Chapter 3

Beginning Your IoT Project

In This Chapter

- Starting small
- Designing an effective pilot
- Checking out two case studies

As Chapters 1 and 2 confirm, IoT offers a wide range of possibilities for a business or government department. But successful implementations need to show operational benefits. They also need to take account of the operational and personnel impacts as well as the technical factors.

Fortunately, we discuss such concerns in this chapter. We describe how to start out and pilot your IoT solution so that it moves seamlessly towards implementation, and we provide two successful case studies to inspire you.

Deciding on Your Starting Point

Although IoT has the potential to transform a business, your starting point needs to be focused, most probably on the area of operational efficiency. You can then extend this start to look at new services and ultimately business transformation.

So start your IoT solution small and then scale up into a larger enterprise solution without having to start again. Here are some typical areas worth considering for a pilot:

- Increased efficiency from monitoring, control or maintenance of a remote asset
- Improved supply chain or other operational processes
- Better actionable insight (see Chapter 1) to deliver improved management of the existing assets being monitored — better maintenance schedules, to give one example

Figure 3-1 shows one example of an IoT implementation strategy.

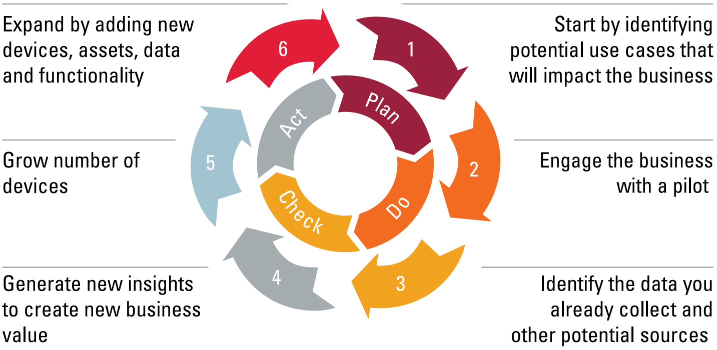
Expand by adding new devices, assets, data and functionality
6
1
Start by identifying potential use cases that will impact the business
Plan
Act
Grow number of devices
5
2
Engage the business with a pilot
Check
Do
4
3
Generate new insights to create new business value
Identify the data you already collect and other potential sources

Figure 3-1: Devising an implementation strategy.

Taking Flight: Piloting Your Project

When designing a pilot, the user interface design is important because, put simply, it needs to be usable, enhancing productivity for the user and supporting the operational demands of the business. You need to consider the potential impact on staff work experience as part of this process and their familiarity with new devices or the analysis that the service will provide. These considerations need to inform the technical decisions made around the pilot.

You can then use the output from this analysis to define the following:

- An outline of the desired outcomes and benefits from the implementation
- An understanding of the specific user case(s) that needs to be initially piloted
- The scope of the technical work required in terms of devices to be deployed, choice of communication service and user interfaces/analytics required, plus whether any further integration is required

Then you can assemble the necessary project team.

Make sure that your pilot solutions are easily scalable into full enterprise-grade deployment so that you don’t need to recode a pilot prior to full rollout.

At the heart of IoT is the requirement for the same environment to host multiple applications with common functions, such as data processing, and alerting shared between them. This design enables your organisation to develop a roadmap for its business that matches closely the operational demands. Doing so negates the need for speculative investments in technology because you can test the value of a solution early in any programme.

Solutions based on IoT require the bringing together of a number of diverse technologies to deliver a specific solution. Therefore, you may need to draw in specialist partners for communications, sensors and data scientist skills to complete a project whilst, at the same time, using off-the-shelf solutions (such as cloud storage and processing) to enable easy post-pilot scaling.

Reading Two Inspirational Case Studies

In this section, we outline two case studies that help you see how organisations can approach the adoption of IoT. Return to these examples periodically as an encouraging reminder of what IoT can achieve!

Going up in the world: ThyssenKrupp Elevator

ThyssenKrupp Elevator is one of the world's leading lift manufacturers, maintaining more than 1.1 million elevators worldwide. The company wanted to gain a competitive edge by focusing on reliability, and so it teamed up with Microsoft and CGI to draw on the potential of the IoT.

CGI developed a solution that securely connects to the cloud ThyssenKrupp's things: the thousands of sensors and systems in its lifts that monitor everything from motor temperature to shaft alignment, cab speed and door functioning; the data they gather; and the PCs and mobile devices its workforce of technicians use. The system captures and combines data into a single dashboard that enables instant diagnostic capabilities via rich, real-time data visualisation.

Now, instead of just reacting to a failure alarm, technicians can use real-time data to define a needed repair *before* a breakdown happens. Plus, thanks to a two-way flow of data, technicians can remotely put a lift into diagnostics mode, or send it to another floor. The result is less time spent travelling, better efficiency and reduced costs, vastly improving operations.

The solution allows ThyssenKrupp to offer something its competitors don't: predictive and even *pre-emptive* maintenance. CGI's solution also uses Microsoft's Azure Machine Learning (Azure ML) IoT service to give ThyssenKrupp an unprecedented view into lift operations and maintenance, now and in the future. The system contains an intelligent information loop: Data from lifts is fed into dynamic predictive models, which continually update datasets. The result is dramatically increased elevator uptime.

Lighting up the streets: Arkessa

Arkessa, a leading connectivity and managed services provider, is working with the Integrated Infrastructures & Processes Action Cluster (IIPAC) to enable the Humble Lamppost project.

Between 60 and 90 million lampposts are estimated to be in use within Europe today, of which 75 per cent are over 25 years old. This figure alone equates to an annual energy cost of €3 billion.

REAL WORLD

The Humble Lamppost is a future cities project that seeks to replace approximately 15 per cent of the existing lampposts in Europe with energy-efficient LED smart upgrades. Their location on the street and the availability of power make them excellent hosts of public safety and communications access services such as CCTV, Wi-Fi, Air Quality measurement and Transport monitoring. In order to reduce the amount of time and energy required to deploy, install the new lampposts, they'll be built to use existing electrical wiring. To enable the clustered services wireless, Internet connectivity will be built in.

The smart cities initiative has been thoroughly embraced throughout the planning and creation stages of the Humble Lamppost project, which has resulted in the devices becoming part of an integrated city model, with collaboration resulting in adoption of open standard protocols and components which will improve services, reduce costs, and also enable cities to work together in order to aggregate demand.

Graham Colclough, leader of the project and chair of the IIPAC, states that the Humble Lamppost "offers many cities a practical way to kick-start their smart city journey".

Arkessa's multi-network connectivity and management services will be the platform on which the lamppost and clustered services are provisioned and managed from a network perspective.

The multi-network capability removes any dependency on any single Mobile Network Operator (MNO) meaning each lamppost can connect first-time to the best network service available in its specific location. This flexibility and robustness also applies to the communication paths courtesy of advanced but standard data networking techniques. In a similar way, mobile and internet security protocols authenticate and secure device registration and two-way communications with a centralized management service.

This approach removes the need for wiring, takes cost out of deployment and is inherently scalable in a massive way. The sheer scale of IoT deployments means automated and remote management is essential. EmPort is Arkessa's secure data management tool suite which supports monitoring, control, reporting and remote diagnostics of connections. Connections can be tailored to suit the data bandwidth and security needs of services deployed on any given lamppost, likewise the tariffs.

All of this is delivered in a single platform and through a single virtualized portal regardless of which MNO service a lamppost connects to or which regions or districts they are deployed. Integration with preferred Enterprise business systems is possible or Arkessa can provide management services on a customer's behalf.

Andrew Orrock, CEO of Arkessa, defines Arkessa's connectivity platform as being agnostic to the underlying communications technology and allows you to monitor, control and manage all of your connectivity in one place. Arkessa makes IoT build out easy in technology and business terms by offering a single service entity regardless of communications provider or technology employed. Arkessa is working with CGI to future-proof Enterprise connections to the IoT.

Chapter 4

Getting under the Skin of IoT

In This Chapter

- Dealing with the core elements of an IoT solution
- Implementing IoT successfully

By investigating what lies under the skin of IoT — its anatomy — you'll find things that are familiar and other things that are new to you. What matters is how it all hangs together.

In this chapter, we define the common elements necessary for building your IoT solution and help you to understand what each aspect includes. We also provide recommendations on what to consider in any design and some perspectives on the appropriate approach to adopt to ensure efficient implementation.

Assembling the Components of an IoT Solution

Figure 4-1 identifies the four required elements when creating an IoT solution. You can put together these blocks in different ways. In this section, we discuss these elements and illustrate each one with an example.

We explain in Chapter 2 how IoT can shape the operation and citizen experience of the city of the future, and we extend that theme here, using the simple example of a council that needs to reduce accidents on residential roads.

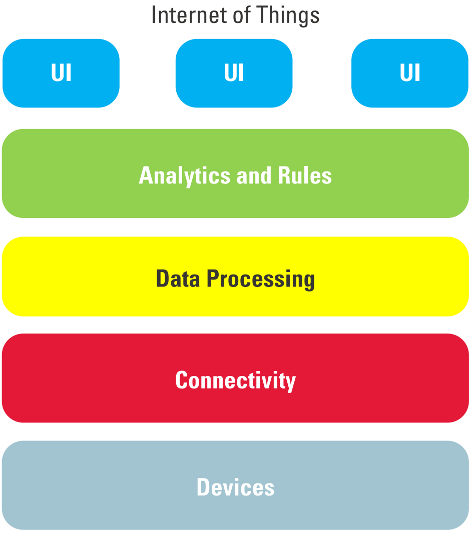

Figure 4-1: The functions required for an IoT solution.

The council is aware that ungritted roads are a big contributor to accidents, and they need to ensure that bins containing grit for the roads in cold weather never fall below 10 per cent when frost is forecast. So, to deliver an improved outcome, operations need to be set up that involve council call centre staff, resource managers and citizens. Monitoring a bin alone (an M2M solution) is part of the solution, but is not enough on its own. To optimise the council's performance, it needs to bring different data sources together. That is an IoT solution.

The following list explains what this IoT solution might look like in practice.

- **User Interface (UI):** This information is what users see on a screen. It contains information relevant to them and is displayed on a device suitable for their use of the service (PC, laptop, tablet, smartphone and so on).

  In this city of the future, the operations centre agent needs to benefit from a variety of data sources — traffic, weather, emergency services — and the relationship between them, displayed in a way that helps to manage events while they occur as well as anticipate demands through access to predictive analysis derived from historical information.

In this example, citizens need their own UI with the ability to check when a grit bin near them was filled and request a refill if the bin is empty. The council needs a UI that lists bins likely to need filling, produced each day, including an emergency list of bins that grit lorries must visit.

The later section "Interacting with users" contains more useful info on UIs.

- **Analytics and Rules:** Each of the different actors in this scenario — council staff, lorry drivers and citizens — need to have the right information delivered to them. The data, coming from different sources and devices, needs to be analysed so that the various actors can use it appropriately. Some data may indicate an alarm state, whereas other data may need to be placed in storage for access later or used to predict future events. Making all this work requires the system to identify which users are permitted to see what information.

  This kind of capability is part of the security needed in IoT, and you should design it in at the beginning of any implementation; don't leave it as an afterthought or wait until a breach has occurred. Security is clearly important and has wide-ranging implications, so much so that we dedicate the whole of Chapter 6 to it.

  In the grit-bin example, to begin to gain the critical insights, a manual analysis is necessary of data from refills over the last five years, compared with frost/snow falls. It's also necessary to compare the use of grit with demographic data for an area, such as the locality of schools, number of pensioners and so on.

  This analysis shows that in any area, key sites exist where more grit is used than others, and they have to be monitored for their levels. For the rest, a simple Near Field Communications (NFC) tag that allows people to order with their smartphones is sufficient because individual orders can be extrapolated. Additionally, the analysis shows that a small number of bins need filling about twice as often as others. These areas should be fitted with a second bin. The understanding that emerges from such insights can drive a new operational model.

  For much more information on this area, check out the later sections "Setting the rules" and "Analysing data."

- **Data Processing:** A high volume of data needs to be processed to deliver the different insights that the various actors need in this example. The data will be coming from different sensors and be carried by the different communication services. Data formats will vary, and there will be a variety of communication protocols, which all need to be managed and handled appropriately. At this point, security needs to operate as well to recognise obviously fraudulent data or attempted hacks, and to pass through legitimate data to storage or for immediate processing.

  So the system requires the ability to analyse data coming through and to decide where it needs to go in near real time, as well as the ability to support a wide range of data inputs from devices. (We provide more details in the later "Processing data" section.)

  In our example, the solution needs to have the benefit of sensor data and source data such as weather and demographic information. The operations centre requires an even broader spread of data sources, including schedules and timetables at a minimum.

- **Connectivity:** The choice of appropriate communications from a device and the sensors associated with it is driven by a number of factors in terms of location, environment, and the type and volume of data that needs to be collected. When implementing an IoT solution, these factors need to be understood in the context of the use case required to ensure that the chosen approach delivers the required user experience. For further information, flip to the later section "Defining device connectivity requirements."

  Simply collecting data from a device in the hope that it may be useful can overload a system and cause costs to rise unnecessarily.

  In the example, not all bins need the same communications or access to near real-time data with the same frequency. This insight drives the adoption of different communication methods.

Considering Important Issues When Implementing Solutions

In this section, we describe the process of implementing IoT. An agile delivery model is often applied (see Chapter 5) where the solution is delivered a feature at a time and, when possible, through active engagement with the intended users. But the steps we describe here are equally valid for agile or more conventional software development where user requirements are documented at the beginning of a project and the technical team delivers to this specification.

TIP

Following this model ensures that you maintain focus on the business benefits, which are key to IoT projects. It also permits parallel development because the interfaces are clearly defined for testing and allows refactoring of the UI solution without affecting the rest of the delivery.

Formulating your goals

You need to have measureable and achievable business goals. Without them, IoT is a solution looking for a problem, and the benefits are hard to track.

TIP

Design your goals in a way that allows key metrics to be used to define the success of the implementation. The greatest success is where a single master goal can be broken down into manageable objectives and milestones.

For example, in the maintenance arena, a master goal would be zero downtime outside maintenance windows. This target would then drive a number of small goals. Each goal is then considered for its impact on development. The master goal would need a calculation of unplanned downtime costs and how often they occur in a time period, giving a potential value for a solution. If the IoT solution costs more than the savings to be made, clearly it isn’t the right solution!

Interacting with users

The business goals of the preceding section feed the UI and use-case development. The UI is the point where users interact with the system. Therefore, the success of an IoT implementation rests on whether the generated insights can be successfully shared with the users.

Ease of use

WARNING!

When the UI is hard to use, it isn't going to be widely adopted. This observation is very important because many M2M projects have started with devices and data and carried out a bottom-up design that ended with information overload at the UI and limited take-up. Where one of the user groups is a client — Customer Relationship Management (CRM) or the public (transport) — this is extra critical.

TIP

Thanks to the mobile app revolution, the expectations have increased, and users don't accept "functional" interfaces with poor looks or ergonomics. Whether it's web-based or an app, the UI needs to be as "thin" as possible and contain only the minimum required to support the user. Logic and data processing are handled in lower levels, allowing you to modify the apps as required and to carry out rapid customisations for particular user groups.

User requirements

Starting from the business goals, use-case breakdowns provide the information and insights that users require to meet each business goal. In a use-case, each point external to the system being developed is an *actor.* So, in addition to the end users being actors, any external IT systems such as CRM or fault management are also actors. A complex IoT deployment contains a number of actors, each with the need to receive or see different information relevant to their role.

After designing the insights, you need to add the interactions. Then you can consider the presentation and define the layout, from which UI development can start.

REMEMBER

You need to consider three outputs from the UI work:

- **Insights:** To drive the analytics work.
- **Use-case breakdowns:** To drive rules and policies.

- **Application Program Interface (API) definitions to supply apps:** So that different code routines can talk to each other — in this case, how the application talks to the rest of the platform. The format is of the form “get insight,” making it easy for developers to deliver the UI required by users.

Setting the rules

REMEMBER

The rules control the functions required to deliver the use-case(s) defined for the UI (see the preceding section), including the policy control to deliver the necessary security. The rules are core to everything that occurs in the solution.

Policies provide security for the solution. Security in IoT is complicated due to the number of individuals involved and the fact that insights have a number of dimensions (see Chapter 6 for more on security). The issue isn’t as simple as whether an actor can request information on an insight but also involves the geographical area, timescale or level of detail. The apps shouldn’t need to know this detail and rely on all calls to return the information relevant to that user. The rules and policies need to take the request and deliver the appropriate response.

Consider the example of maintenance. Engineers need to know the next site to visit, and the UI requests it. The rules and policies know that users are allocated a geographical area, what equipment they’re authorised to work on and their current location. The system returns information on the next site based on this and the selection rules.

Analysing data

REMEMBER

Analytics starts with a manual phase, which is driven by manual analysis and mining of the available datasets in order to answer the following questions:

- What raw data is required to generate the insights required?
- How much of this data is already available?
- What additional data is required and at what frequency?

- What algorithms are needed to drive the automated generation of the insights?

IoT works on multiple time frames:

- **Real time:** A decision and action have to occur in less than 1 second and are usually carried out in the device.
- **Near real-time:** A decision and action have to occur in less than 1 minute; drives the majority of rules and interactions.
- **Batch processing:** Where the processing of intensive analytics is carried out. In many cases, the outcome of the batch processing is a simple algorithm that can be run in real time with little processor load.

  An example is machine learning. Training the machine learning function can take a long time, but when the model is trained it can answer queries on new data coming in rapidly. The challenge for the analytics team is to find the right analyses to produce these simple algorithms.

REMEMBER

The output from the manual phase drives the development of the production algorithms, which run at different levels within the system. Trigger points for near real-time alerting need to examine the data as it comes into the system *(data in transit).* The daily run to calculate assets that need servicing runs off stored data *(data at rest).*

Defining device and connectivity requirements

When the UI and analytics work has defined the data required and the frequency of collection required, you can define the device requirements. By working top-down to the device requirements, the decision on complexity of device is driven clearly from the business goals, and the additional cost can be shown if a more complex device is needed.

This is the benefit of being driven by a business goal approach. Simply rolling out devices and then seeking to find value in the data produced results in undue complexity, which leads to key parameters being missed.

WARNING!

The drawback with devices is that, in many cases, they can't be reconfigured easily. For example, when fitted, a smart electricity meter has to last 15 years in service, so when considering the costs, potential on-site engineer visits need to be factored in. Plus, if cellular or another radio communication service is required, you face ongoing service costs, which need to be managed, and so the volume of data sent needs to be kept to what is essential for the solution.

Processing data

Data processing glues all the other functions together. IoT pulls data from a wide range of sources, such as devices, external entities (weather reports, traffic updates) and a number of internal databases. This data needs to be arranged in a form that other systems can efficiently ingest without additional processing.

REMEMBER

This requirement leads to the concept of *streams* being used in IoT. High-volume data feeds are sent through a stream processor, which splits and pre-processes the data so that it's ready to be consumed. This approach compares with more traditional, processing-inefficient solutions where all the data goes into a so-called data lake and each consuming function has to dip into the lake.

TIP

After you move to a streams-based approach, you can run a lot more of the analytics functions on the data in transit. At each step, the data is enhanced until you're handling insights rather than raw data. The need remains for archiving raw data for future manual analytics, but you can optimise that for long-term storage.

Chapter 5

Delivering Your IoT Solution

In This Chapter

- Thinking about your approach to implementation
- Making the journey

Chapter 4 explains the different functions that need to go into your IoT solution, but here we talk you through preparing for delivery, including getting your goals clear and getting the most from your solution. We then let you in on some useful tips to make your IoT life a whole lot easier.

Preparing for Implementation

From a high-level business view, IoT comprises three key parts:

- Devices and the data they collect
- Actionable insights generated from this data
- Workflows that leverage these insights in order to provide business value

REMEMBER

To implement your new IoT capability, the starting point is the business value and the interactions needed to create that value. These aspects drive the required insights and any new data that you have to collect. As we discuss in Chapter 4, simply rolling out devices without an understanding of the business goal can be a costly mistake to make.

You need to be able to answer the following questions:

- Who needs the new insights and in what format?
- What workflows will be created or changed?
- What are the business outcomes?

Following an example implementation

Here we use an example of a company that offers maintenance services.The business was aiming to change how it sold its services, moving away from the conventional contract service level agreements (SLAs), which were measured on mean time to repair (MTTR), to availability measures based on a prediction model.

The client wanted to investigate two key steps:

1. **Learn from the historical data already available to size the IoT project.**

   This step covers the gathering and analysis of existing data, manually at first and then combining it with other existing data that has already revealed insights in order to understand why parts had failed and what was the cause. The types of data collected includes *event measurements* (number of times a mechanical part has moved), *condition measurements* (temperature of oil in pumps) and alerts from the control system.

   Combining all this data produced two datasets:

   - List of most likely faults based on alert history
   - Measure of the expected life of components based on service history

   These two datasets were combined to see the alignment and to find “quick wins” in the system. As expected, the 80:20 rule (also called Pareto analysis) holds true in that just a few parts caused 80 per cent of faults.

This analysis also provided pointers on additional information to be collected and information that didn't have great value. As a result, the company could pursue an implementation approach based on an understanding of required investment costs and device capabilities for data gathering, as well as ongoing running costs. This ensured that the investment matched the information needs to meet the business goal.

2. **Enable a new business model based on availability rather than MTTR.**

   As new data becomes available, there is a need to integrate the IoT solution with other systems and update workflows to deliver the information that underpins the new business model. Over time, this expands to cover a wide range of existing systems, from purchasing to HR, but initially it's done in small steps, working with business users and focusing on maximal business benefit for the expenditure in early phases.

   The user can then measure each incremental change and identify easily the point of diminishing returns.

REMEMBER

A part of each development is the User Interface (UI). In some cases, you can use the existing system as a front end.

Collecting actionable insights

After you've implemented and realised your core business value, you can gather a wide range of additional insights, often as relatively simple incremental additions.

For example, if a mechanical assembly or electrical part is removed in a repair, it's usually returned to the supplier or an internal workshop for testing and repair and, if possible, put back into spare part stock. In some cases, the part tests okay on the bench and is marked "no fault found." This approach incurs expense for several reasons:

- The root fault hasn't been fixed, and so another engineer visit to the site is likely to be required.
- The shipping cost of the part.

- Most spare part supply contracts incur a fee for no fault on returned parts. This cost falls on the organisation performing the maintenance, not the end client, but it's unlikely that anyone beyond the team that deals with spare part stock and returns sees it, and so the end-to-end cost of these mistakes is certainly not considered.

By pulling this additional data into the analysis, you can not only consider the cost (and potential savings) but also use other factors, such as engineers involved, service areas and equipment types, to generate a full root-cause analysis.

These incremental changes also help you to drive product quality, indicating where, for example, local conditions require different materials.

Appreciating the Advantages of Agile Development

Understanding the different development approaches you can take to an IoT project can be useful, so we provide a summary here.

Traditional software development projects involved a formal collection of requirements from the business, which would then be documented before the project team was tasked to produce a solution based on agreed timescales and after appropriate testing. Changes in scope or modifications were considered as change requests.

The adoption of cloud-based services and rapid development tools has encouraged the adoption of agile methods. Agile methods enable developers to work more closely with the ultimate users of a system in terms of UI and features. Projects are usually made up of short pieces of development called *sprints*.

IoT projects are ideally suited to this approach, given the importance of user engagement and the UI experience for the success of the project.

Clearly, new solutions can be developed using more traditional approaches, and some scenarios justify the investment in bespoke on-premise solutions. But adopting an agile approach, working closely with business users and building on cloud technologies can drive increased benefits from IoT technologies, as we describe in this section.

Reducing time to market

A number of application development platforms, used with agile development principles, are available in the market. These allow real pilot deployments to start in less than 6 months and at around 10 per cent of the cost of traditional development. We guess that got your attention!

Common functions are made available so that the support architecture does not have to be designed and built from scratch, and projects can concentrate on building the solution required.

Delivering benefits

REMEMBER

Adopting a business benefit driven approach is important to getting "early wins" and buy-in from the business. An agile development approach is ideal for supporting this objective.

You also need to keep an eye on costs. In an enterprise rollout, a number of costs will exceed the cost of the IoT solution itself, for example:

- **Installation costs:** Take account of the cost of installing new devices/sensors, or even a wide-ranging firmware upgrade, on an existing plant. The cost of engineers' time on-site can easily be two to three times the cost of the hardware.
- **Integration costs:** Integrating into the existing IT estate is necessary, but can be costly.

Validating the benefits

WARNING!

In order to optimise the benefits of your IoT solution, you need to have methods of measuring the gains from the new insights. As soon as you lose the ability to measure or calculate what the system is providing, you run the risk of not getting the return on investment anticipated in the business case.

REMEMBER

Ensure that you drive each sprint to develop a new workflow or capability from a clear understanding of its value. At the same time, make efforts to ensure that the new insights are available for the wider organisation and that they enable further benefits.

When new consumers of insights are onboard, new use-cases and requirements are sure to arise. These aspects will drive the roadmap, which is where an agile approach wins. Above all, get buy-in; the more people who are excited about a development and see its value, the more benefit your organisation derives.

Starting small

The initial data gathering and analysis without any new technology allows you to understand what you need to measure. Afterwards, run a small-scale trial to test and prove the technology with "low hanging fruit" before moving to a wider rollout. Performing development in small increments allows you to add new features regularly and measure the incremental benefits immediately — a win-win!

Chapter 6

Securing Your IoT

In This Chapter

- Introducing the security concerns
- Knowing your enemy
- Constructing a system with security in mind

Naturally, you want to keep anything of value as safe as possible, whether it's at home or work. You wouldn't leave your house doors and windows wide open, and you need to think along the same, safe lines for digital threats.

Cyber security is an ongoing issue for most organisations and their IT systems — and the IoT is no exception.

Many organisations separate their computers and networks from the Internet, implementing firewalls and intrusion monitoring at the connection to the Internet in order to prevent and detect attempts to access their internal computers and data. Larger and regulated industries also increasingly implement additional security mechanisms within to prevent internal users from damaging or impacting systems.

In this chapter, as the advertising slogans have it, we take your security seriously! We describe the types of threats you face and how you can combat them.

Understanding the Nature of the Threat

Sensors and devices used to send back telemetry from a remote physical location or monitors of a patient's vital signs were previously connected to a computer by a bespoke and ageing protocol over serial links such as RS232. But today they're connected via well-understood protocols, such as TCP/IP, across the Internet directly to computers at the heart of the corporate environment.

As a result, these devices are potentially reachable via the Internet from anywhere in the world, and therefore potential targets of a cyber security attack. Flip to the nearby sidebar "I'll crack that system in 4!" for some facts and figures.

Whereas devices used to work within benign closed systems with proprietary and specialised computing devices and protocols, now attacks are exposing the ease with which they can be disrupted.

For example, in 2008 a group of researchers demonstrated the capability of an attacker to control remotely an implantable, wirelessly connected cardiac defibrillator and to determine the level and timing of the shocks to be applied to a patient. In 2011, another group uncovered and disclosed techniques to access remotely and exploit, via the mobile phone network, a car's internal electronic (engine management) system by generating control messages on the internal car network.

Scary stuff. Therefore, just as the office computing environment migrated its security measures from the perimeters of the enterprise or office network (with firewalls and monitoring systems) to the individual computing device, so too must IoT networks and devices take measures to protect themselves.

I'll crack that system in 4!

Over the years, the Internet Storm Centre has tracked the time before attackers can compromise an unpatched operating system directly connected to the Internet.

Varying from approximately 20 minutes in 2003 to 4 minutes in 2008 to 40+ minutes in 2012, the statistics mirror the addition of protection to the network and operating systems security — and not, unfortunately, that the statistics show the number of attacks being launched is slowing.

Thinking about Ways to Keep Your IoT System Secure

IoT, by its very nature, means that many devices are connected via the public Internet in publicly accessible places. Therefore, as part of struggling to control access to the devices themselves, you also need to protect against the oldest of security threats—theft and physical tampering with the device.

Even if some devices don't store large quantities of data locally (and many such as electricity smart meters can), they potentially do provide access to the network, and are often (wrongly) trusted devices as part of a wider corporate IT system, reaching deep into the corporate network.

Typically, the attacks with which you need to concern yourself fall into two types:

- **Those that access the device while it's still running:** This type is best illustrated by recent security researchers who were able to reprogram a connected smoke alarm with a USB stick and load their own software on it.
- **Those accessed when the device is turned off or disconnected:** Here attackers physically open up and tamper with a device in an attempt to extract the data or often use secret keys to encrypt messages or data stored on the device. They access the electronics of the device itself, sometimes the testing or diagnostic circuitry (JTAG connector) or simply the embedded processors themselves. Some have even gone as far as imaging the chips themselves to work out the encryption used in some smart meters.

In both types, the challenge of IoT devices (with their limited memory and computing power) is to either protect those interfaces or encrypt and minimise the data they store. The implication is to never assume that these devices are always trustworthy.

Staying safe

With many devices now being embedded into industrial and consumer systems, ones that were previously believed to be secure can become insecure (over time) with the discovery of flaws (missed and built-in many years ago) and new methods and techniques of exploiting systems.

The application of software updates or patches by many software vendors to fix these flaws after they're deployed is well understood and publicised for software such as Microsoft, Apple and so on. Indeed, mobile phones have also applied software updates Over The Air (OTA) for a number of years.

Similarly, the challenge for IoT devices is to ensure that these updates can be developed and applied in a timely manner (especially because attack code can and has been generated within hours of the public disclosure of the vulnerability). However, the constraints for IoT devices may be different because devices often have low power consumption requirements, and minimal computation power and memory, so that process has to be efficient.

Some devices can't simply afford to stop processing for 15 minutes while they update and then consistently reboot multiple times until the patches are applied. Imagine what could happen if those devices were controlling a processing plant or medical equipment.

Also, sometimes the problem is not changes to the software but to the configuration information used by the device. You need to have methods for ensuring that only the right people can change this configuration and that you don't open it up to attackers being able to change settings. The "Stuxnet" attack on Iranian nuclear processing facilities shows that this threat is real and not just something shown in blockbuster movies.

If you can't stop attackers from tampering with your device or attacking it, you need to be able to detect when they're doing it!

Unlike a traditional corporate system, IoT has some potential advantages over traditional corporate security monitoring, namely that the traffic from devices is often more simple and well defined. The industrial process sensor often has a predictable pattern of data and connectivity; outside of those parameters, it's easy to spot the rogue device and take action against it.

Preparing for an attack

As for corporate systems, the increasing numbers of cyber attacks have taught organisations that it's not a case of if you'll be attacked, but when. The challenge for many organisations is how to respond and manage that incident response.

The attacks can take two forms:

- **A denial of service *against* your IoT solution:** For example, compromised devices could produce a flood of readings that stop the solution from receiving the data that it needs.
- **A denial of service *using* your IoT solution:** For example, an attacker can hijack many of your devices and generate traffic to slow down, say, a banking website or industrial control system, or maybe just generate spam email. This has already occurred in a smart fridge!

There are important security questions to be answered when you're designing your IoT solution, and you need to consider these from the outset — not as an afterthought.

Chapter 4 explains the different layers that make up an IoT solution. Each of these needs a robust security approach in its own right, but it is also important that there is an overarching view of the whole system.

A multilayered strategy needs to be adopted to address the question about what happens when there is an attack, and not just deal with prevention.

Addressing security, data privacy and access rights from the beginning ensures that the solution will be scalable and adaptable to the evolving needs of the organisation.

Building a Secure IoT Solution

Given the difficulties of maintaining a secure IoT system, a compelling case exists for putting together a system and process that puts security first. This requirement means securing the devices, the back end and the protocols used to transfer data and instructions, and ensuring that effective process and security-aware people are around the system.

REMEMBER

Although many security concerns are focused on attacks from unknown or external attackers, don't lose sight of the fact that your trusted suppliers and employees (who access these devices and analytics platforms to maintain or operate them) also have the potential to cause damage. This was the case in 2000 when an ex-employee remotely controlled a number of devices to send sewage into a clean water supply.

Understanding the threats (physical, electronic or regulatory) is a vital step in developing an IoT system because it allows you to analyse the architecture and place the security controls at the right location (for example, on the device, in the network or at the heart of the analytics platform to protect the system and its data).

TIP

IoT brings significant security challenges with many traditional security controls, such as encryption, potentially making integration difficult or weaker than intended. This does not mean that these can be ignored as being 'too hard', but the whole system — from 'thing' to end user — needs to be designed to be secure.

TIP

Validate all such claims by purchasing and sourcing from a well-established secure supply chain. Also, security test these systems before they're deployed and on an ongoing basis to avoid the emergence of any additional flaws.

Chapter 7

Ten Handy Hints for IoT Success

In This Chapter

- Targeting your IoT effectively
- Getting help from experts

In this chapter, we provide the ten parts of the IoT Holy Grail! Follow these tips, and your IoT project is far more likely to run to plan, saving you a lot of unnecessary stress in the process.

Starting Small and Scaling Up

Your IoT project needs to start in the specific areas of your business where you can clearly identify real business value (Chapter 3 has more on this aspect).

Because IoT has so many potential applications, it is important to focus on the first step that will give you most value. If you adopt the approach recommended in this book, you can handle adding further devices and services in an incremental manner.

Focusing on Insights that Impact Your Business

Use workshops to engage the business and technology to identify how near real-time business can positively impact your organisation.

As with the adoption of any technology, understanding how it will benefit both employees and customers is essential. The workshop can be an opportunity to help business management and operations to understand the process and provide input into the desired outcomes of a pilot.

Flip to Chapter 2 for loads more on the possible impacts of IoT.

Using a Pilot Approach

Pilots play an important role in validating benefits and forming a basis from which to build IoT solutions that deliver value to the business as a whole. They need to be more than simply a proof of concept.

Ensure that your pilot proves the overall business case and can be developed as a core for future development. Check out Chapter 3 for much more on what an effective pilot project looks like.

Developing a Roadmap

Creating a roadmap for your IoT deployment that integrates across your technology landscape is invaluable.

IoT solutions inevitably bring together IT and operational technology, link to customer relationship management (CRM) and so on. Therefore, your roadmap needs to reflect these connections.

A roadmap enables the business to prioritise the different solutions that will need to be delivered to realise the anticipated value from an IoT investment. It also provides a means to assess the extent to which each deployment meets the defined success criteria and lessons that could be learned for further rollouts.

Identifying Companies to Help You

A third party (and we mean suppliers and partners, by the way) has an important part to play in delivering your IoT vision.

They can be specifically helpful in the provision of specialist skills and experience — for example, data scientists and advanced analytics.

A number of elements go towards building an IoT solution. Although inside an organisation, or with a single supplier, many of these skills and capabilities may exist in part, drawing on specialist experience, and knowledge in this new area of technology will mean less learning on the job and avoid denting confidence through projects that are only partially successful.

Adopting an Agile Approach

Embracing an agile, “fail fast” development approach ultimately delivers an improved return on investment.

In adopting new technology, you may be tempted to keep hoping that another version or update will make the difference. In taking an approach that focuses on clear, achievable outcomes, assessing potential success and not wasting time vainly hoping for a new development becomes easier. This “fail fast” approach allows you to come back to previous ideas as the technology advances, as it will do, at an appropriate time while you make a success of what is available now.

Chapter 5 is the place for more information about agile development.

Engaging Business Users Early On

Employing effective user interfaces (see Chapter 4) to gain business users' engagement from the start is important; in fact, it's the key to success.

They need to be able to see what information can be delivered to them and used for their benefit, especially in a time when users of systems are increasingly influenced by the experience they have in using consumer technologies such as smartphones, tablets and so on.

Showing future users what screens may look like and the information they could contain helps not only with their engagement but also with the success in meeting business outcomes. Their input is also a source of real understanding of how the organisation actually works in practice rather than in theory!

Learning from the Experience of Other Businesses and Collaborating

Collaboration can speed up IoT development and reduce cost of deployment.

Finding new ways of sharing information and knowledge and forging new forms of partnership enables businesses that work together (for example, in a supply chain) to take advantage of new technologies where each party can benefit from the investment.

Keeping Abreast of Technology and the Art of the Possible

The development of technology in the IoT space is rapid; what was impossible a year ago may become possible in a relatively short period of time.

The different technologies that make up IoT — cloud computing, sensors, communications and data analytics — are all evolving in their own right, improving usability and performance, but also how they interact together. It is this improved inter-working that will offer the best opportunities for step changes in capability and the potential for new services.

Working with an Integrator

An *integrator* (that is, a firm that takes responsibility for putting together all the building blocks of an IoT solution) can help you create an IoT end-to-end experience. Its role can vary from managing the development to making partner recommendations to offering a fully managed IoT service.

FOR DUMMIES®

CGI's highly successful *For Dummies* series with Wiley includes the following titles:

Smart Metering Implementation Programme For Dummies

GB Water Industry For Dummies

GB Electricity Industry For Dummies

Implementing Enterprise Asset Management For Dummies

New Nuclear For Dummies

Smart Grids For Dummies

Smart Metering For Dummies

GB Gas Industry For Dummies

The Internet of Things For Dummies

To download or request a copy of any books within the *Dummies* series, visit **www.cgi-group.co.uk/the-dummies-series** or email **enquiry.uk@cgi.com**.

The Internet of Things (IoT) explained!

The Internet of Things For Dummies is your essential pocket guide to the latest and, arguably, most disruptive technology development that businesses are facing today. This book explains, demystifies and summarises the key challenges and opportunities that IoT can bring to enterprises.

- ***Get an overview of IoT — understand the origins of IoT, how it applies to different industries and how it will shape the future for business and consumers***
- ***Learn how IoT is being implemented today — through real-life case studies and scenarios, discover how IoT isn't just an idea…it's happening now***
- ***Appreciate what it takes to deliver IoT securely in your organisation — find out how to get your organisation behind an IoT initiative with a "start small, but start" approach***

Open the book and find:

- **What IoT actually *is***
- **What IoT means for businesses and government**
- **The difference between IoT and other technologies, such as Machine to Machine (M2M)**
- **How security is a vital component in IoT solutions**
- **How IoT implementation is about bringing together a team within the organisation and using skilled partners**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

John Hicklin, Bill Shurvinton and **Gemma Beard** are key members of CGI's IoT team.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-04330-0
Not for resale