CANONICAL

Defining IoT Business Models

Monetising IoT investments, maximising IoT skills and addressing IoT security

July 2017

HIGHLIGHTS

- For many businesses looking to take their first step into IoT, how to start and the benefits are unclear.
- This report examines 3 key elements; **how IoT can be monetised**, **what skills are required** and **addressing fundamental security concerns**.
- 361 IoT professionals contributed their experiences and opinions on the current state of IoT plus future challenges and opportunities.

From the connected factories of Siemens and AirBus, through to smart home products of Samsung and Bosch, the Internet of Things is providing businesses with a whole new platform upon which to build innovative products, processes and new business models.

With a current market valuation of over $900bn[1], both manufacturers and those looking to adopt IoT solutions are well aware of the potential of IoT. However, in trying to leverage this potential, many business are still grappling with how IoT can benefit their business and the best approach to get started with their IoT initiative.

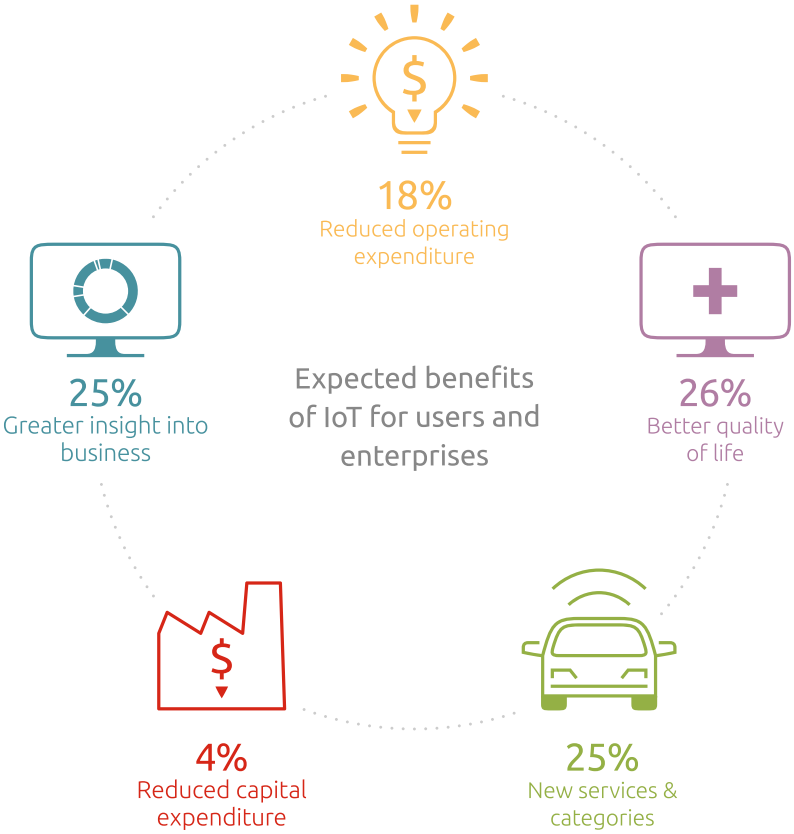
Canonical recently commissioned a survey to examine exactly these questions. It looked at the views, opinions and experiences of 361 IoT professionals regarding past, present and future IoT projects.

[1] McKinsey&Company, 2016

The IoT Dilemma

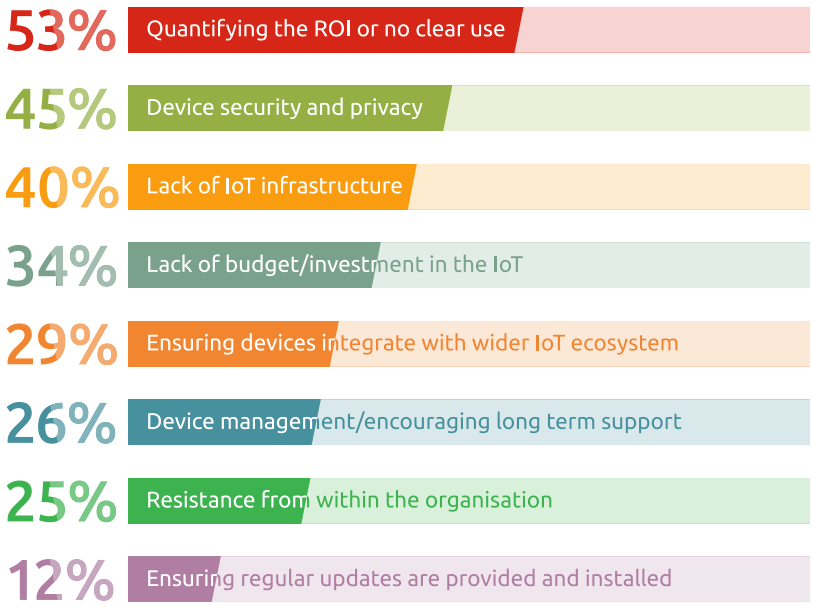
Businesses see massive opportunities in IoT, but are also aware of significant challenges

Broadly-speaking, respondents to Canonical's survey see a number of basic ways in which the internet of things might benefit the business community:

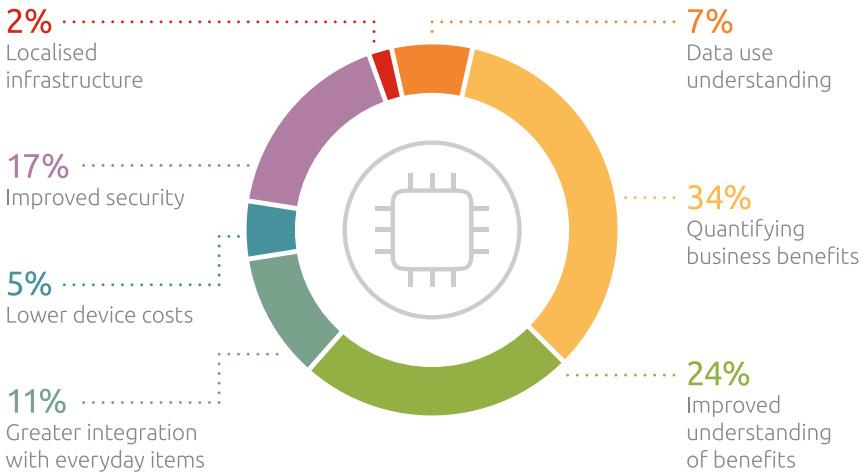


While a quarter of IoT professionals are focused on the opportunities offered by new connected products and services, just as many are excited by the potential big data insights that connected technology could provide their brands.

These same professionals stated that the most immediate challenges they are faced by IoT are:



Similarly, when asked what they believed was needed in order to encourage IoT adoption among enterprises, the top priorities to emerge were:



While IoT professionals recognise the potential of IoT, it's clear that they believe the underlying business case and how to get started implementing IoT needs to be better understood. The above findings indicate not only concerns about security, as to be expected, but also how they set up an IoT ready organisation and how to turn their investment into one that can drive new revenue growth. In addressing these points, this report will answer three simple questions:

1. 'How can IoT investments be monetised (and justified)?'
2. 'What skills are needed in order to develop and maximise IoT solutions?'
3. 'How can the industry address the issue of IoT security?'

55%

of IoT professionals see their profits coming from the sale of hardware

Approaches to monetising IoT

Many organisations are struggling to understand what many would argue to be the most important question in IoT – how, exactly, will they make a return on their investments? This section will look to explore the different routes to monetisation and which may be most wise for the long run.

Many vendor companies will continue to profit through hardware sales

As it stands, 55% of IoT professionals see their profits as coming from the sale of hardware. And with hardware revenues continuing to go up, driven by the sheer volume of hardware required by the IoT, these hardware vendors can be confident of the fact that they will continue to make decent money for some time to come.

With chipsets and electronics dominating the cost of IoT devices, it's a natural place to explore when trying to determine the future of IoT hardware. With every generation of IoT hardware, we are witnessing an increase in processing ability, a reduction in size, and ultimately, a significant reduction in cost. As electronic hardware becomes cheaper year after year it potentially means lower bills of material and higher margins for hardware vendors.

The reality however is very different. The pressure of commoditisation means that without product differentiation, the downward pressure on price is stronger than the reducing cost of the bill of material. This leaves hardware vendors with little choice; either choose more expensive custom components with a price premium and serve less price sensitive, niche markets, or use commoditised components and try to differentiate.

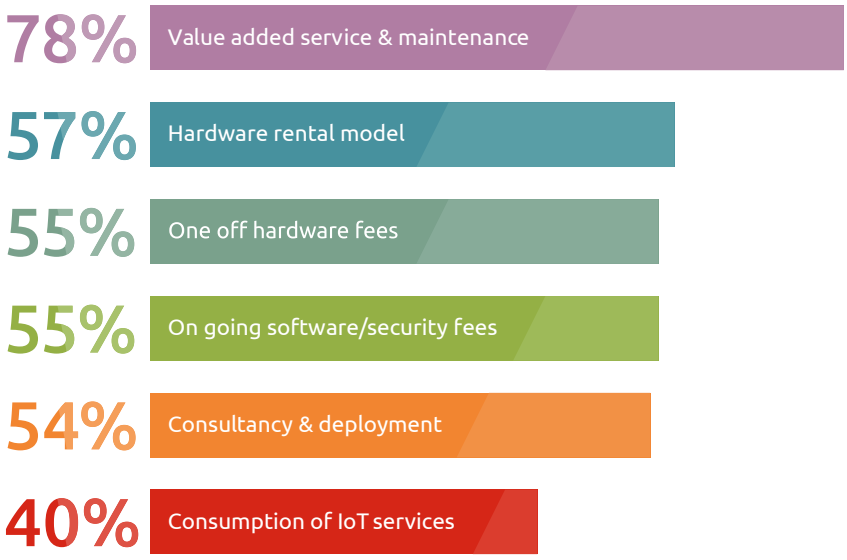
This second approach is the one chosen by an increasing number of IoT device manufacturers, turning their backs on bespoke hardware solutions and choosing instead to fit their devices with fully general-purpose single-board computers (SBCs) or system-on-chips (SoCs).

Where once the idea of running a full computer rather than a simple microcontroller would have been viewed as overkill (both in terms of cost and functionality), as the size and price of SBCs such as the Raspberry Pi or Orange Pi has plummeted, developers can now justify using them as a low-cost, high-power alternatives at the heart of all of their IoT devices.

So how are IoT businesses looking to differentiate and turn profit in the Internet of Things?

Monetising IoT

Expected monetisation methods of IoT



Profit will be increasingly driven through services and software – which are also potential monetisation routes for owner/operators

The results from the survey question above speak loud and clear with IoT vendors exploring a number of new business models to complement hardware and envisaging that the sale of software and services promises greater revenues. We can see that the overall percentage[4] of IoT revenue represented by hardware is on the decline. 78% of IoT professionals agree that the real monetisation of connected devices will lie in the creation, deployment and maintenance of value added services, with 40% stating it will be, specifically, through the consumption of services. With the exception of consultancy services, all the other monetisation models are from scalable productised services. And the only way to deliver these services is through embedded or cloud software which effectively turns a hardware product into a 'thing as a service'.

This shifting of the value centre sharply towards software is rendered possible only by the commoditised electronics available to hardware vendors. In a world where all compute can affordably be general-purpose, the functionality of virtually all devices will be defined by the software running on them. But this shift of value also needs a change of approach from device manufacturers to put software right at the heart of their product.

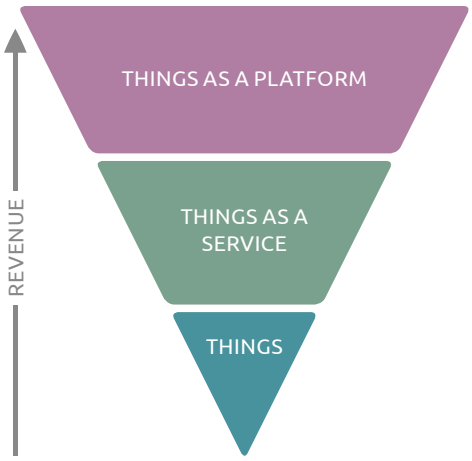
[4] IT Wire

This valuable new avenue for monetisation can only come from a connected device using a general-purpose-compute SoC/SBC, that treats software, not as a one off component that ships with the hardware and never changes again, but instead as an essential part of the product that will evolve over time and that can be bundled and monetised in a number of ways. This starts with the operating system and extends all the way to the business specific applications being run on the device.

As a result a versatile, IoT specific operating system such as Ubuntu Core, that can be repeatedly upgraded and has the ability to add new functionality in the form of apps plays a key role to opening up the IoT to new based software business models

Software business models: 'And the rest…'

There are a number of additional business models at play in IoT today, including:



Things as a platform

- Revenue from industrial insights: for example, sale of failure analysis stats gleaned from industrial machinery
- Revenue from personal insights: similar to the above but at a consumer level, for example, the sale of anonymised fitness tracker data
- Revenue from 3rd parties creating applications for your hardware

Things as a service

- Support: for example, repairs resulting from the prediction that a device will require maintenance could result in the device-owner saving money further down the line. Repairs can also be directly monetised, and can result in improved brand loyalty
- The use of IoT devices for context-specific advertising
- Value from the interaction of human factors and machine interaction: for example, warning a consumer when their device detects it is too close to a source of danger ('pay per warning")

The opportunities that these business models present to device manufacturers are much more attractive than the old hardware opportunities. However, migrating to these approaches requires a mindset shift from hardware manufacturers:

	Hardware approach	Software business model approach
Products	Physical goods	Virtual goods and services
Channel	Face to face	Online sale only
Lifecycle	Infrequent software upgrade	Continuous integration and delivery
Product management	Hardware design	Service design
Value chain	Integrated	Working with 3rd parties through APIs

This is a paradigm shift not dissimilar to the one the consumer software industry went through when migrating from shrinkwrapped software to app store business models.

The Orange Pi App Store

Orange Pi maker Shenzen Xunlong Co. recently launched an app store for its Orange Pi SBC – based on the award-winning Raspberry Pi SBC. This store, based on the whitelabel app store offering from Canonical, gives developers a simple mechanism to share their snaps (a universal Linux application packaging format) with the wider Orange Pi community. This app store has been driving adoption of the Orange Pi, fostering an active ecosystem, giving developers access to powerful development tools, and providing a route to monetisation for both developers and Shenzen Xunlong Co.

Profiting through IoT app stores

An 'app store for things' is the natural extension of the app store concept. But rather than being applied to software applications running on a phone they apply to any new software based service that can be offered on a 'thing'.

App stores for things have the following characteristics:

- They can be used to distribute any type of software-based service: new functionalities, reconfigurations, analytics and so on
- They offer an online sales channel
- They take care of the software distribution without any effort from the developer
- They can be used to distribute securely any software, whether internal or 3rd party
- They can be 'white labelled' to offer services specific to the device they are installed on

Through the development of an IoT app store, businesses can offer add-ons and enhancements to their existing connected devices, charging users to download and install packaged applications to build upon their existing IoT technology. Such stores represent an opportunity not only for vendors, but also for software vendors and system integrators to widen the market for their software and services.

This software sales or app store approach is set to fundamentally change the way that businesses benefit from investments in the internet of things, with 55% of IoT professionals saying that they intend to monetise their devices through the use of ongoing software-led upgrades.

The 'app store for things' can be used in a variety of ways. For example, Lime Microsystem, producers of mobile base stations, use a white label appstore from Canonical to let base station owners configure their device in one click and turn a 4G base station into e.g. a powerful Wi-Fi hotspot. Lime Microsystem uses the fact that the configuration file that makes the hardware a 4G base station or a Wi-Fi hotspot is only a piece of software, and packages that configuration file as an application that can be downloaded from a store.

InnovaPoS: Using IoT to deliver new and innovative vending services

The smart vending machines market is on the rise with estimates of 2.7 million to be sold by 2020. InnovaPoS[5] operates over 30,000 smart vending machines for big brands such as Coca-Cola, Audi and LVMH in more than 120 countries, either retrofitting existing machines to make them 'smart' or create new ones with advanced features ranging from Wi-Fi hotspots to facial recognition or high-definition touch screens. By connecting machines to the IoT and integrating 'smart' functionality, InnovaPoS is enabling new, monetisable use cases ranging from remote stock management and maintenance, through to individualised advertising, gamification and social networking.

It is also worth bearing in mind that, while the term 'app store' is usually associated with paid third party applications, it is also possible for companies to use an app store as a simple yet effective distribution mechanism to distribute their own software – either as a means of delivering upgrades or to patch devices en masse in-the-field.

In a world where every connected device generates data, the opportunities for monetising this data are limited only by your access and your imagination. We're likely to see a number of until now unpredicted methods of monetisation emerge as the industry develops further.

It is this approach that Canonical promotes through its growing work in the IoT space, encouraging the adoption of a single IoT operating system[6] upon which advancements and new functionalities can easily be developed and delivered via snaps.

This is the future of the IoT – a future of software defined everything. But in the same way that companies require new approaches to software distribution to approach the IoT they also need a new set of talents.

[5] InnovaPOS
[6] Ubuntu Core

The Internet of Talent: Identifying, and hiring, the right skills

Of course, there's little point choosing a business model or technology unless you have the capabilities necessary to deliver on them. Many businesses are concerned by their own lack of knowledge and skills within the IoT market. With high potential for profit and low barriers to entry, widespread promotion of the internet of things has led many technology brands into a gold rush of IoT investment and product design. Unfortunately, given its relatively new status, many business leaders have found themselves running headfirst into a set of technology and business challenges that they do not yet fully understand. What they need is a new generation of talent with the knowledge and skills to navigate the current Wild West that is the internet of things.

"The evolving architecture in the IoT landscape is rapidly moving from basic end-point devices delivering data to cloud applications to a more diverse and complex computing model. This means that in addition to the need for data science and security skills, that are in short supply, distributed computing skills are also emerging as an important requirement. Any current 'full stack' developer or architect now has to be aware of many more components, it may be anything from machine learning, Artificial Intelligence or Blockchain to new user interfaces such as Augmented Reality or communication stacks on emerging networking protocols. The physical world presents design challenges too, where time of day, remote locations or weather conditions can alter the ability to operate reliably.

This technology wave also presents organisational challenges where IoT projects often cross boundaries and silos – we see tension in the industrial sector between Operational Technology (OT) and IT departments where each claim ownership of IoT. The instrumentation and control of physical processes belongs to the production line, power station or oil refinery, where edge analytics drives improvements, yet the enterprise applications and aggregation of all the data in the cloud belongs with IT.

This also applies in smart cities, where street lighting improvement offers cost savings in power consumption, but the infrastructure can also be used for traffic management, parking applications or pollution sensing, which are unlikely to be the responsibility of the lighting department. Enterprises need to consider how to bring groups together to gain the ongoing benefit of business opportunities that emerge which could be done by extending the responsibilities of a someone such as a Chief Information Officer."

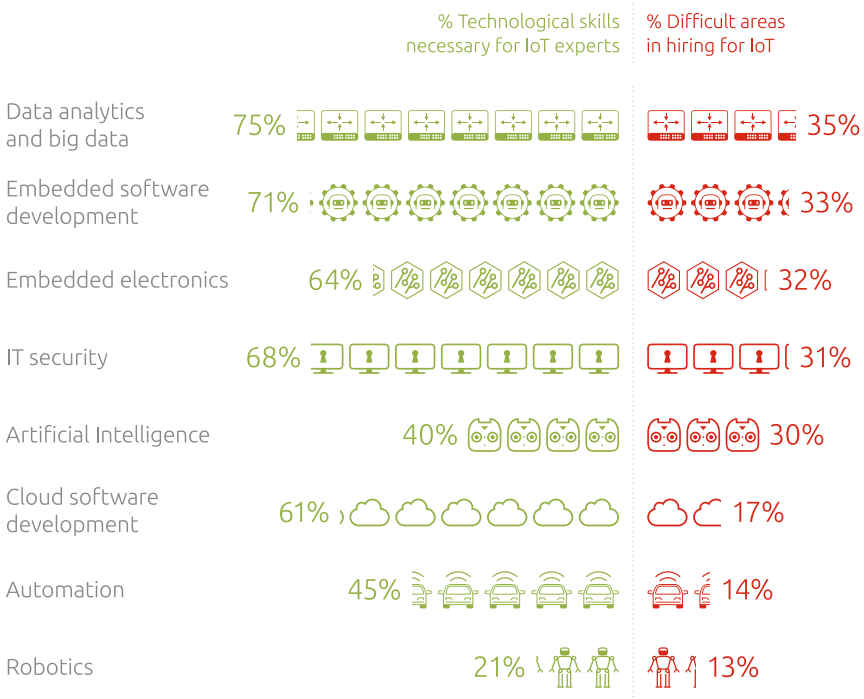
Ian Hughes, Analyst – Internet of Things
451 Research

Finding the right skills

The first question that an organisation looking to embrace IoT needs to address is what skills they require and whether any of these already exist in-house. The sheer scale and scope of IoT means there is a plethora of skills that could be required depending on the project or projects within an organisation. The requirements for these may vary and evolve over time, meaning that organisations need teams who are multi-functional and thus generalists by nature but also cover a number of specialisms across the entire software stack from low level embedded code to machine learning capabilities in the cloud. Inevitably some of these skills will be commonplace already but IoT will also increase the need for skills that weren't previously required.

To this point, Canonical's research revealed that 68% of IoT professionals are struggling to hire employees with IoT skills, with the hardest skill to hire for being Data Analytics and Big Data (according to 35% of IoT professionals) - a skill critical to gathering, analysing, and potentially monetising the vast amounts of data produced by IoT devices.

Hiring the skills for IoT



33%

are struggling to hire employees with embedded software capabilities

It's not just cloud development talents that are required. When asked what skills they deemed necessary to be an IoT expert, after data analytics (at 75%) software development skills were found to be the most needed skill (according to 71% of IoT professionals). In one sense this is surprising, as embedded development is by no means a new discipline. But when considering the fact that hardware is rapidly commoditising, with monetisation and differentiation increasingly coming from software, it is natural that businesses invest in building up their embedded software development capabilities. Unfortunately, 33% are struggling to hire employees with this particular skillset.

What are the IoT jobs of the future?

According to a number of sources ranging from Techcrunch to CIO, the most likely new positions driven by the IoT across businesses will include:

- The CIoTO
- **The IoT Business Designer** The individual responsible for determining unexplored business models and processes is likely to command a premium
- **'Fuller stack' developers** Increasingly employers will value developers that can offer everything from UX to cloud skills, and everything inbetween

Also, we're likely to see an increase in demand for positions such as:

- **IoT Architects** Compensating for the increasing architectural complexity of IoT stacks
- **Data designers/data scientists** Looking to extract value from huge amounts of data generated by IoT devices
- **Chief Data Officers** The need of ready access to data access will increase concomitantly with increased data volumes overall
- **Machine learning specialists**
- **Security consultants**
- **Mechatronics engineers** For developing human/physical machine interactions

While the long list of job titles offered in the 'IoT jobs of the future' section might seem bewildering, the reality is, especially in an industry as dynamic and fast-changing as IoT, that attempting to see more than a couple of years into the future is extremely difficult and most companies aren't in a position to hire at scale. Fixed costs become too prohibitive especially for those in the early adoption stage of IoT where the value and ROI to be derived is still questionable or has not had chance to prove its full worth.

Therefore once an organisation has identified the skills they require, consideration needs to be given as to whether some or all of these skills are better outsourced at least in the short term. In addition to overhead advantages, there is also the benefit of bringing in expertise from individuals, consultancies or system integrators who have significantly more IoT experience to aid the implementation while sharing knowledge throughout the business.

During the process of identifying the skills that are required and whether to build these internally or source externally, businesses will inevitably encounter a number of questions which they haven't had to face before – some of which have already been addressed.

Other considerations that need to be taken into account in this new world include:

- Who is best placed within an organisation to lead IoT projects?
- Who is best placed to bridge the gap between the complex technologies involved and the need to create profitable business models?
- What new roles will be created and which may soon be surplus to requirements?
- Will the traditional IT department continue to exist or will it be more of a hybrid function combined with other departments?
- What is the risk in waiting to make changes versus acting now?

While these questions might sound daunting, a number of software development and IT department rules are still going to be valid now and in the long run. The choice of software development stack is one. By choosing a software development stack that can run as easily on the edge of the IoT network as in the cloud, companies will benefit from code reuse but also from being able to use the same developer across the stack. This is particularly true in the new world of IoT where gateways run similar software as the cloud and where heavier development languages can be used at the edge thanks to increasingly powerful IoT chipsets. The choice of operating system is another one that has a huge effect on operational costs. Once again choosing an operating system that can be used from the edge to the cloud means devops, support and security engineers can integrate the new IoT operations much faster in their workflow.

Above all, businesses must adopt an iterative and agile approach when it comes to deciding on the right people, skills and team to take them forward into their internet of things world. It is unlikely that what is decided upon today, will remain the same in even one or two years, so constantly being in a position to evaluate what requires changing and being able to execute this quickly is a must. This underlines the need for a team of individuals who have a broad range of skills and can adapt quickly. It is also another argument for why businesses should consider running proof of concepts before jumping all-in to give themselves a chance to experience and understand what works and what doesn't before they scale too high and possibly in the wrong areas. And finally, this is a good reason for businesses to adopt IoT technologies that have flexibility and upgradability at their heart.

Of course, it won't matter how sound your business model is, or your skills base, unless you've worked out how to keep your devices secure in-the-field…

2 out of the top 3

worries around the current state of IoT related to security, with lack of agreed security standards (67%) and poor security (54%) being the primary concerns

Over 50%

of IoT devices are unsecure, believe the majority of IoT professionals asked

Effective management of IoT security

The last half of 2016 saw an explosion of high-profile, headline-friendly IoT-related security issues. In September 2016, the world witnessed its largest ever IoT botnet attack through Mirai; a string of malicious code which, through the co-opting of vulnerable devices, brought down a swathe of ISPs and online services affecting businesses and consumers alike. The root cause was traced to devices using factory set default usernames and passwords.

It doesn't take a great deal of imagination to see the potential outcomes of such attacks. More recently, the WannaCry ransomware worm was responsible for a number of high profile exploits of outdated, unpatched Windows XP desktop systems – including several used by Britain's National Health Service – resulting in a number of high profile ransomware demands. How long before IoT is exploited in similar ways?

- In 2016, over 23,000 news stories were published concerning the threat of IoT security
- 21% of IoT professionals surveyed by Canonical believe IoT security issues have been overly 'hyped up' by the media
- However, 79% disagree, believing that the media has either portrayed an 'accurate' picture of the IoT's security issues, or that they had actually been underplayed, and would be 'much worse than they think'

The genie is out of the bottle as far as IoT security is concerned. As hackers get ever more interested by the swathe of poorly protected IoT devices, it seems likely we'll see more such attacks take place, with malicious agents utilising swarms of IoT devices to compromise commercial entities.

Tackling IoT security effectively, and thereby minimising risks, is therefore critical in establishing a clear business case for IoT among enterprises.

What are the risks?

The potential risks to businesses from poor IoT security are considerable. It's impossible to provide a comprehensive list, and exactly what those risks are depend on whether you are an IoT device manufacturer or a company using IoT as part of your business to drive operational savings or offer additional services.

On the whole, IoT device manufacturers face the prospect of heavy fines, legal action, and brand damage if their devices don't meet acceptable security standards. In early 2017, for example, the Federal Trade Commission sued Taiwanese network infrastructure firm D-Link for failing to secure its devices against the Mirai IoT botnet attack. While the proposed fine reached as high as $16,000 per device, over a quarter (26%) of the IoT professionals we surveyed claim that they would have liked to have seen an even higher fine introduced.

However, it is businesses using third-party IoT devices and services that arguably stand to be the real 'victims' of IoT security violations. Like manufacturers, they might face fines, legal action and brand damage, but also data loss/theft and industrial espionage, denial of service leading to revenue loss, access to their private audiovisual feeds and violation of staff privacy, etc. The risks associated with incursions into critical business systems, as enabled by IoT devices, hold the potential to be catastrophic for IoT adopters.

Offsetting IoT security issues

So what can be done to mitigate the risks to businesses from IoT devices?

Maintain an accurate audit of all of the IoT devices as they are installed: It's hard to guard it if you don't know it's there. And with the potential for (often tiny) IoT devices to be situated anywhere on the inside or outside of a building, mounted on street furniture or buried underground, they may be hard to audit after-the-fact. Record the locations, technical details, passwords and technical specs associated with each IoT device as it is integrated into your network.

Vendors and users must ensure simple best-practice, such as secure passwording, is in place on devices: Ensure that no devices are running with default administration passwords, and even better use key based policies to limit access to the device. As much as possible, restrict physical access to devices. Ideally, the OS running on these devices will go some way to mitigating against default passwording and the dangers of physical access.

Enterprise IT departments should ensure their on-premise IoT devices have appropriate access permissions set up: To prevent anyone from deliberately or accidentally introducing malicious code or behaviours via devices that are already connected to the corporate network.

Updating of devices should be regular, seamless and, if possible, automatic: One of the best defences against security incursions is to ensure the most immediate patches are applied as soon as they become available. Operating systems built for IoT like Ubuntu Core are able to apply digitally-signed 'over-the-air' patches to devices in a centralised, no-touch manner, ensuring devices will always be up-to-date.

Mitigate against the potential failure of the vendor company: Sadly, the rate of failure of young IoT companies is high. Both vendors and users of devices need to consider whether IoT devices have a potential update path in the event of security patches being halted by the vendor company. Using operating systems like Ubuntu Core, which have a clear and standardised delineation between code provided by the vendor and code provided by the user, provides a route whereby the user can easily find an alternative device or can find a support to maintain the device's code in the event of the vendor company's failure.

57%

of IoT professionals support the standardisation of IoT software/infrastructure as a means of ensuring better IoT security

Ensure IoT devices run an IoT OS that is built from the ground-up for security: Overall, you should look for an on-device OS that treats security as a primary concern. As well as providing automatic security updates Ubuntu Core will roll-back the software and data to the previous working version should an update fail. It also features entirely read-only, immutable applications, and defaults to preventing any interactions between on-device apps (snaps) unless those interactions have been rigidly pre-defined.

In the medium term it seems likely that the industry will respond to escalating IoT security threats with a mixture of government-mandated legislation and network-level security. However, it is Canonical's view that the first and most effective point at which security should be addressed is the on-device OS – specifically, through adopting a security-first IoT OS, on which the same codebase and practices as the standard enterprise security measures can be applied.

Conclusion

While IoT security and the recruitment of IoT experts remain major points of concern for both vendors and developers alike, on the list of immediate challenges facing the IoT community, these remain secondary only to quantifying ROI and finding a clear use case for the internet of things.

Many business leaders simply don't understand how the IoT will benefit their organisation, and as such have little incentive to take the risk of investing in a technology, particularly one that may not be 100% secure. If however, organisations take significant steps to educate themselves regarding potential business models, and to grapple with the immediate challenges of building capacity and knowledge while maintaining security, there would be a far greater push towards innovation, collaboration and investment in the IoT.

How the business world can extract value from the IoT over the coming years is a broad and complex question, and there is no 'one size fits all' answer. As this report has demonstrated, there are a couple of key areas that need to be explored as a priority, such as how a business makes money, who are the right people to lead, and how to ensure security is at the heart of everything. Once these three areas are established, any business will have a far better grounding in which to benefit from IoT.

Four ways to get your organisation IoT ready

The internet of things will offer near endless opportunities to today's businesses, impacting everything from industrial manufacturing through to high street retail. While there is still a long way to go before many businesses are ready to truly embrace IoT across their entire organisation, this report has highlighted several ways that they can get started, adapting their thinking for the new connected age.

With this – and the findings of Canonical's research – in mind, here are four initial steps to get your business started on its journey towards effective, and profitable, IoT use-cases:

1. Think strategy, not just products

Making the jump into a new IoT-led business model means so much more than just connecting processes to a dashboard or converting existing products into "smart" devices. An effective approach to IoT must look beyond connected products and start to strategically consider all the ways how the internet of things could improve profitability throughout an organisation. This could include streamlining services through improved analytics, selling additional services as snaps or add-ons, or simply selling advertising data from existing smart devices. The possibilities for both cost-savings and profit generation go far beyond simple hardware sales.

2. Don't just build knowledge, hire it

The internet of things covers a vast array of technical and business applications, as such it is very difficult for any one individual to call themselves an "IoT expert". Instead of attempting to develop all knowledge internally, business leaders should not be afraid to look beyond their traditional hiring streams and turn to employees and experts from outside of their own fields. According to Canonical's research, everything from embedded software development to knowledge of automation and IT security will prove vital in the age of IoT. As such, businesses must be willing to step outside their comfort zones and learn from a much broader variety of fields.

3. Work with the industry to overcome risks

Collaboration is set to be a key part of corporate IoT adoption. Until businesses learn to work together, set standards and build upon each other's achievements, the internet of things will continue to suffer from the same security and interoperability issues that have plagued it for the last five years. While much of this collaboration will be driven by business leaders themselves, technology will also have a key role to play in ensuring that brands work together to develop a stronger infrastructure for the IoT. Through the use of snaps and IoT specific operating systems such as Ubuntu Core, businesses can guarantee that their products and services are built on a stable, unified platform – offering greater opportunities for collaboration and cross-device developments.

4. Join the dots

Many of the best IoT innovations will not come from a single use-case, but rather from the interactions between different IoT platforms, processes and devices. The profitability of IoT does not lie in devices themselves, but rather in the connections that those devices enable across an entire organisation. Often it is these connections – and the unique insights that lay between them – that will provide the greatest opportunities for profitability and business growth. In order to succeed in the IoT space, brands must be able to spot these connections, using the data available from their various IoT touchpoints to identify weak spots, unexpected cost centres and unexplored gaps in the market.

The internet of things is all about making connections – and that is exactly what businesses must do to monetise their investment in the IoT.

If you would like to discuss these issues in more detail, how to make the internet of things a business reality for your business, or find out more about Ubuntu Core and snaps, you are welcome to contact Canonical at https://www.ubuntu.com/about/contact-us

Methodology

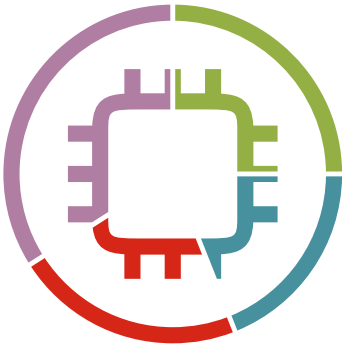
This report brings together quantitative research from 361 IoT professionals as well as qualitative examples and case studies from Canonical's own clients and experiences within the internet of things. The research was commissioned by Canonical, but completed by independent industry publication IoT Now.

Canonical defined IoT professionals as those currently working within the IoT space, whether as product developers, manufacturers, vendors or engineers. Those that do not work in the space were qualified out during the survey.

Our research

Over 360 IoT professionals were surveyed, commissioned by Canonical, and completed by independent industry publication IoT Now.

Developers	34%
Vendors	22%
Enterprise	19%
Other	26%



ubuntu
Delivered by Canonical