KPMG

Security and the IoT ecosystem

KPMG Australia

kpmg.com.au

Foreword

When it comes to the Internet of Things (IoT), you can believe the hype. IoT will likely be bigger than most people think and it presents great opportunities for innovative Australian businesses to lead the way.

But success in the IoT space will take more than slick applications, connected devices and advanced analytics; it will also require a robust approach to security, privacy and trust.

For the technology sector, the message from businesses and consumers is clear: be innovative, be bold and be secure. IoT will bring massive growth to tech companies and IoT developers that can carve out a dominant position in this expanding market.

However, with evolving market maturity and heightened competition has come mounting concern for current and potential IoT users, particularly around security.

This report suggests tech firms and IoT service providers will need to work quickly, diligently and decisively to deal with concerns related to security (how well controlled is the device and the infrastructure?), privacy (how is data kept confidential?) and trust (how is customer confidence being addressed?), before they turn into problems. Those that fail to do so will have a difficult time growing in this new environment.

The technology sector must come together with other vertical and horizontal players in the ecosystem to create a unified approach to security and standards that everyone can live by, and grow with. Today's current state of fragmentation and competition on standards will only result in greater complexity for users and reduced growth for the IoT sector.

This report aims to catalyse the debate and extend the body of knowledge on IoT security. Drawing on a recent global survey of 100 IoT 'user organisations' and supported by one-on-one interviews with industry leaders, academics and KPMG's IoT professionals, it hones in on IoT security, privacy and trust, providing advice for all players in the emerging ecosystem.

Over the coming year, KPMG Australia will take a deeper dive into these key issues. Supported by insights from our global network of technology and IoT professionals, we will explore how these key imperatives are being managed across sectors, applications and ecosystems.

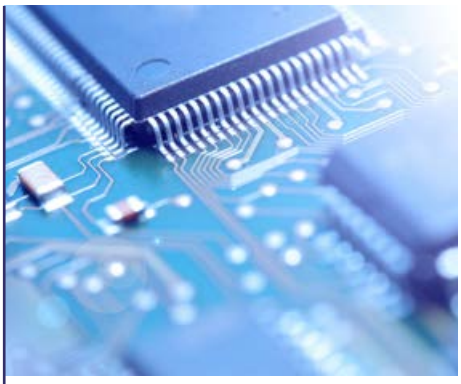
Chris McLaren
Partner
National Sector Leader
Technology, Media & Telecommunications
KPMG Australia

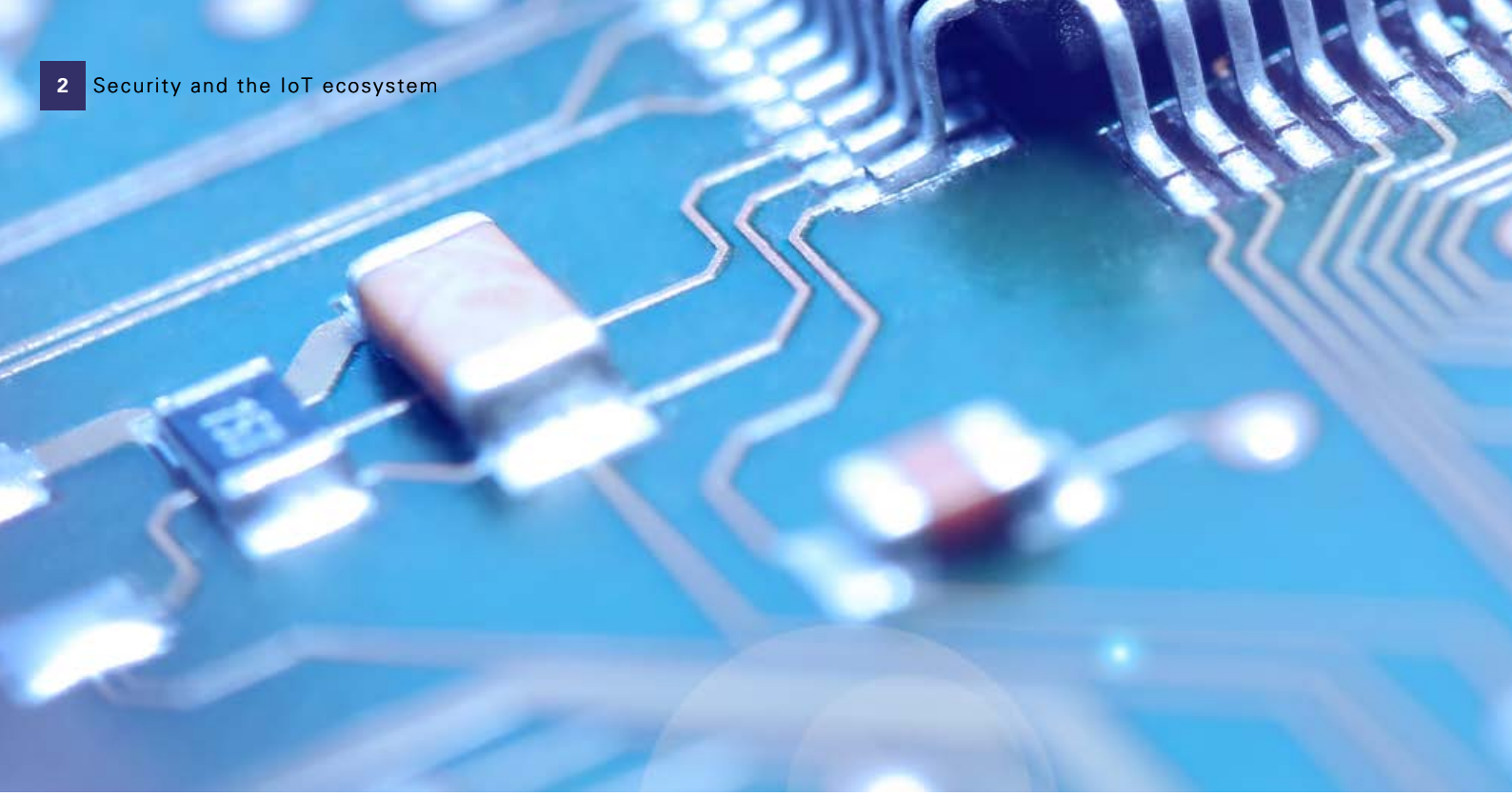
Gordon Archibald
Partner
Cyber
KPMG Australia

The Internet of Things (IoT)

Combining data, cloud, connectivity, analytics and technology in a way that enables a smart environment in which everyday objects are embedded with network connectivity in order to improve functionality and interaction.

Table of contents





Cyber security a 'must have'

92%

of IoT users are concerned about cyber security

Source: KPMG Cyber Security and IoT Survey, 2015

Business leaders may recognise the potential advantages that IoT can offer, but they are deeply worried about the risks. The majority admit that they don't fully understand the cyber security threats that IoT brings.

While IoT customers may not be willing to pay extra for security, recent security breaches in consumer data, devices and systems suggest that they will lose confidence and may even avoid solution providers who fail to take the appropriate measures to protect their security.

Everyone wants to be first 'out the door' with a new IoT solution or product. 89 percent of our survey respondents said they believe that the first movers in IoT will enjoy a clear competitive advantage in their markets. Technology firms and IoT service providers are fighting to get their products out to market faster, eager to capitalise on the massive growth potential.

The rationale is obvious. Those that are able to get to market first and solidify a dominant position in the IoT value chain should be well-placed to parlay their leadership position into rapid and sustainable growth. However, history is littered with products and ideas that placed speed-to-market over quality and value, subsequently losing their advantage to other – less nimble but more robust – competitors.

Companies will need to prioritise security alongside other key considerations such as speed and usability when developing and operating IoT solutions.

Dr Mike Briers, Founding CEO, Knowledge Economy Institute, says the potential economic, social and environmental benefits that arise from digital services enabled by IoT technologies are enormous, but security is key.

"This emerging hyper-connected world, however, brings with it many challenges, not least of which is the need for reliable, safe and secure networks. Trust in these networks is essential not only for service uptake and delivery but also to guard against misuse and disruption especially to critical services".

IoT growth potential

No one doubts that IoT represents a massive opportunity for businesses, consumers and tech companies. Most organisations are just starting to scratch the surface of what they can achieve with IoT solutions.

For device manufacturers and application developers, the rapid adoption of IoT-enabled devices is expected to drive a new round of growth and expansion as the number of installed devices sky-rockets. According to IDC Research, the installed base of IoT units will grow 17.5 percent per year. And within the next 5 years, forecasts suggest that the market will be worth a whopping US$7.1 trillion.[1]

However, as businesses, governments and consumers get more and more familiar with the benefits that IoT can deliver – smart cities, IoT-enabled supply chains, smart appliances, automated vehicles, wearable devices and much more – key concerns around security, privacy and trust are likely to grow.

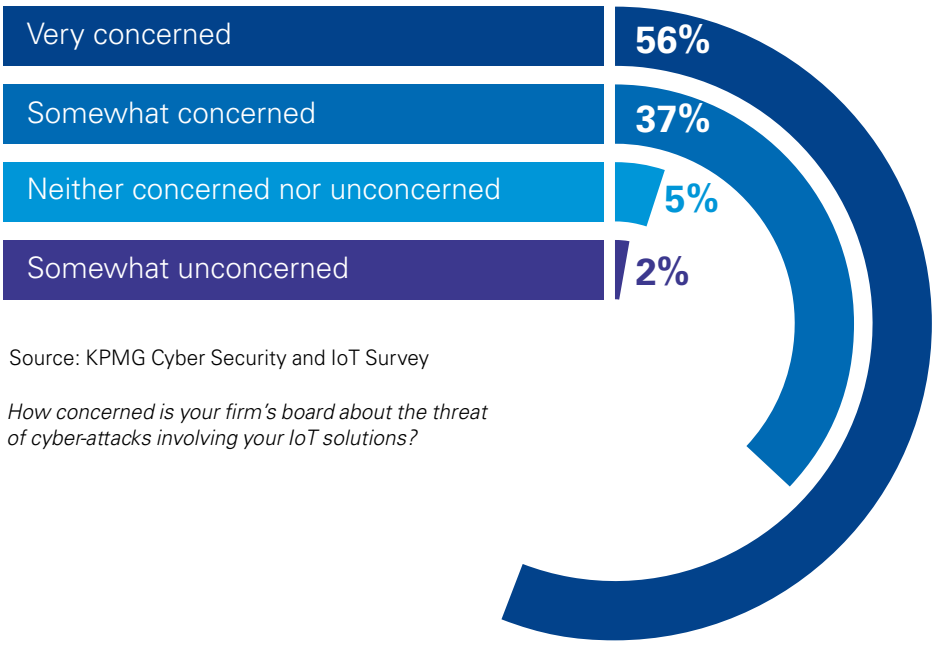
1. Worldwide and Regional Internet of Things 2014–2020 Forecast, IDC Research, 2014

Taking the threat seriously

Corporate leaders of organisations utilising IoT are certainly concerned about the potential impact of a cybersecurity breach within their environment. More than half – 56 percent – of respondents in our survey said that their board was 'very concerned' about the threat of a cyber-attack. More than a third said their board was 'somewhat concerned'.

As one Asia-Pacific-based Chief Risk Officer said, "Our management board is very concerned about the threats of cyber-attacks, in light of the increasing number of cybercrimes and the vast technologies that are employed for IoT solutions. Naturally, the whole IT system has been designed and integrated with new IoT devices, so any threat can be a significant blockage in our business continuity."

IoT users and their boards are becoming increasingly concerned about the risk of cyber-attack on their IoT solutions



Source: KPMG Cyber Security and IoT Survey

How concerned is your firm's board about the threat of cyber-attacks involving your IoT solutions?

Risks and opportunities

While the 'downside' risk can range from data loss through to denial of service or loss of control of a device, improved security in IoT can also provide significant advantages. A robust cyber security stance, commonly accepted standards and strong actions towards earning business and consumer trust will be key to ensuring long-term advantage and, ultimately, supporting growth.

Chris McLaren, Partner and National Sector Leader for Technology, Media and Telecommunications, KPMG Australia, says there are notable opportunities that counter the risks.

"Australia has the opportunity to become a leading user of IoT technology – showing the world how to drive maximum value from IoT," he says.

"However, we do need to focus on the segments that mean the most to us that will drive in-country value plus export opportunity. For example, Smart Agriculture, Smart Cities, and Connected Transport and Infrastructure all seem like priority places for us to focus and create outstanding use cases."

McLaren says IoT presents particular opportunity for Australian start-ups to develop technology and solutions, but challenges industry not to miss the surge.

"As a nation we largely missed the micro-processor wave, the PC wave and the mobile wave from a technology development or creation standpoint – are we going to miss the IoT wave?" he asks.

He says Australian innovators need to overcome the risks and the friction points, namely security issues, and to experiment, learn fast and "look for opportunities to have business, government, technology and education collaborating vigorously".

It is this collaboration that could give Australian businesses a competitive edge.

"IoT will bring maximum value when specialists and best-of-breed technologies come together as an ecosystem to solve the most complex, meaningful problems. It will not work in silos – no one technologist can fulfil the whole chain, and IoT has the potential to cross and remove traditional business boundaries."

He gives the example of collaboration around a targeted business problem, such as using IoT to increase the shelf life of a food produce. An integrated approach could involve micro-sensors in fields to assess when produce is ready, along with a network for communication with the micro-sensors. There would be a platform to ingest the data, a secure place for data storage, an interface to manage the crops, and involvement of the farmers, pickers, logistics companies and store owners.

Kevin Bloch, Chief Technology Officer, Cisco Australia and New Zealand, agrees that IoT opportunities can be best harnessed collaboratively.

"Although Cisco is committing significant resources and investment to IoT and IT infrastructure on a global scale, we cannot do it alone," he says. "We don't make the end-points, the 'things', such as wind turbines, jet engines or even the tags. We also don't pretend to be experts in many of the vertical segments. Therefore we have to work with others, we have to collaborate and we have to partner."

Looking for standards

Characterised by massive growth, wildfire adoption and rapidly emerging use cases, IoT in some respects is a virtual 'Wild West' with few rules, little regulatory oversight, absence of standards and masses of pioneers in competition.

The industry, regulators and users will need to come together to agree on appropriate standards, including for security. Many organisations now believe that the development of industry standards will be the most important step to driving IoT adoption. Indeed, it is often not until generally accepted standards are set that most new innovations truly achieve mainstream adoption.

Knowing this, many technology firms – both large and small – have started to create consortiums of like-minded organisations to help focus on creating and commercialising new standards. These lead to tight competition and significant uncertainty for players in the market.

Examples include Google Nest, which has partnered with Samsung Electronics, ARM Holdings, Freescale Semiconductor and Silicon Labs to develop their 'Thread' networking protocol aimed at standardising IoT communications in the home.

Another example is Intel, which has partnered with Cisco, AT&T, GE and IBM to create standards specific for industrial IoT use. Cisco is also part of the AllSeen Alliance created by Qualcomm, alongside Microsoft, LG and HTC to create an interoperable peer connectivity and communications framework.

The Hypercat Consortium in the United Kingdom is a great example of technology companies, government and business coming together to develop standards for the application of IoT in the Smart City space.

Speed vs. standards

Given the pervasiveness of IoT and the sensitivity of the systems and data, nobody doubts the need for clear IoT regulation and standards. However, there are concerns about the balance between competition and speed to market versus standards.

McLaren says in this changing space, "learnings need to inform regulation".

"For the time being adequate regulations exist around privacy, spectrum and security. However, we need for regulation to rapidly follow innovation – where it is absolutely necessary. Policy at the moment needs to be focused on encouraging innovation, experimentation and government taking a leading role in utilising IoT – whilst keeping an eye to emerging issues that need addressing through regulation."

Increased regulatory oversight and guidance could drive forward adoption. Almost a third of companies already using an IoT solution said that the existing lack of rules and regulations were creating challenges to IoT adoption.

For example, many currently available connected cars have access to an 'auto-pilot' feature which promises to reduce accidents and improve safety. But – to date – road regulators have not "caught up to this innovation" and therefore have been unwilling to allow this feature to be used on public roads, thereby severely limiting the value gained through this technology.

> "The Internet of Things carries the potential to transform industry verticals and enrich the lives of billions of humans, but its potency harbours real risks to network and personal security, while the potential to compromise individual privacy will need to be tackled with creativity and caution. It's a 'taming the tiger' exercise that we cannot afford to shirk or mismanage."
>
> —John Stanton, CEO, Communications Alliance

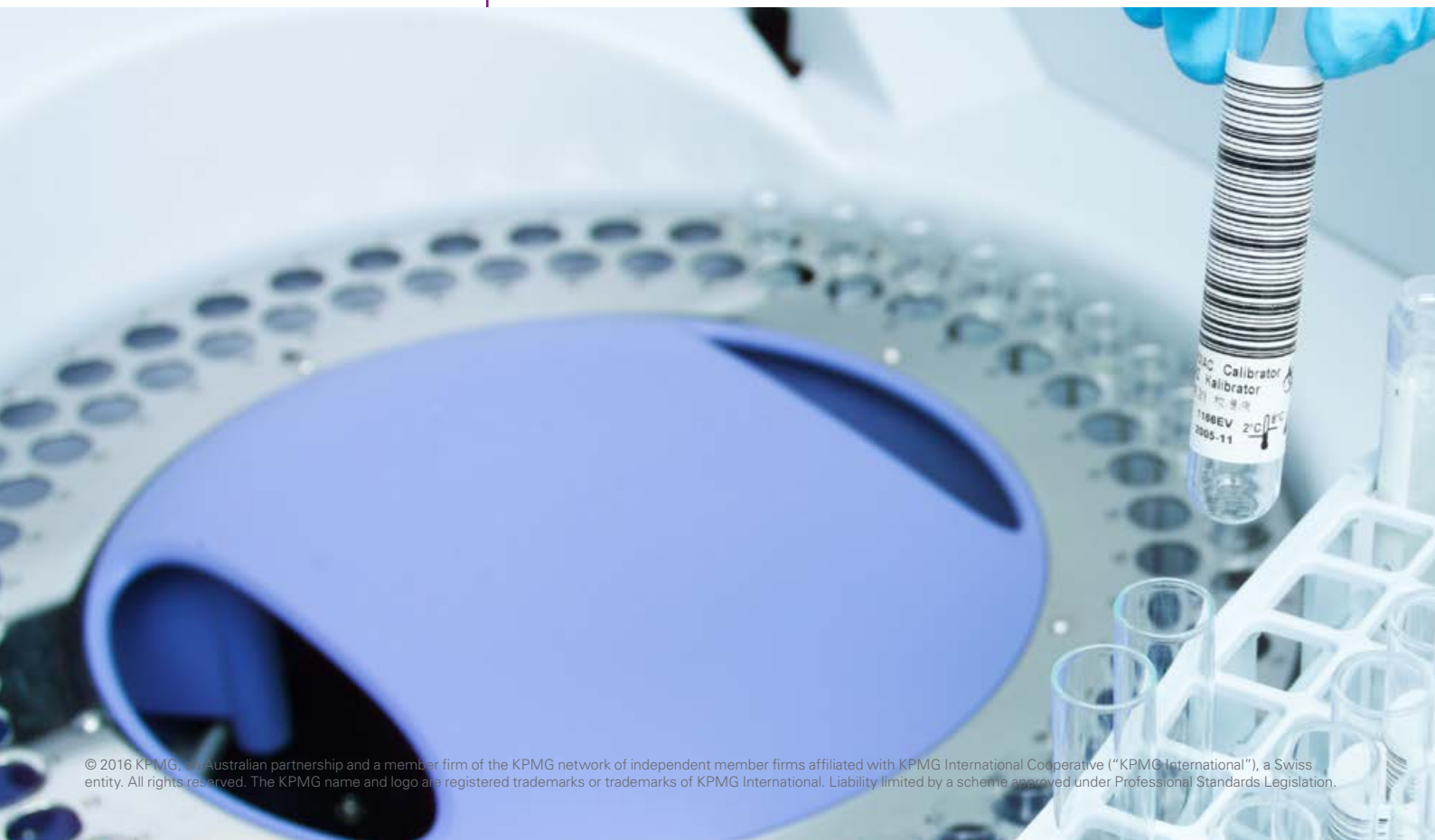
More to do

Few technology companies and IoT solution developers are actively working towards creating standards. Fewer still are engaging with regulators to understand – and to inform – the direction of future regulations.

Malcolm Marshall, KPMG Global Leader, Cyber Security says, "It seems that many of the smaller tech players in the ecosystem are simply standing on the sidelines waiting – along with their customers – to hear what standards and regulations will win the day; they are letting the bigger players make all the decisions."

However Marshall thinks this is not time to take a passive stance.

"Tech firms should be out there working collaboratively with as many consortiums as they can to understand – and, where possible, influence – the various standards being created."



> IoT promises significant opportunities from the sheer volume and variety of data that it will provide to companies. However, that very diversity and volume will bring with it massive challenges for our wireless networks and networking infrastructure. It is vital that companies take a holistic view of IoT applications, ensuring that the full requirements on infrastructure and back end servers are dimensioned and considered.
>
> —Ian S Burnett, Dean, Faculty of Engineering and Information Technology, University of Technology Sydney

Focus on security, privacy and trust

The most successful IoT solution providers and tech companies will likely be those that focus equally on improving security, protecting privacy and building trust. All three elements are key to building market-share in the IoT space.

While the topic of cyber security certainly seems to be front and center for both IoT users and developers, most are taking a rather narrow view of their obligations. A robust cyber security approach focuses not only on protecting the devices and infrastructure that underpin the system, but also on developing the right level of data privacy and building trust with customers and regulators.

What is security, privacy and trust in the IoT ecosystem?

Successful IoT solutions, products and innovations will require tech firms and solution developers to think about three key concepts that enable a valuable user experience: security, privacy and trust.

McLaren says that privacy and security are real issues for Australian businesses in the IoT space.

"Business, government and individuals should always understand fully what technology is being utilised, what data is being captured, where it is being transmitted and stored, who has access to it and what mechanisms are in place to protect it," he says.

Security – an organisation's ability to control their environment, devices and software – is most frequently discussed at industry conferences and meetings. It can often be embedded into coding or manufacturing processes and updated regularly.

Privacy relates to confidentiality and data control and can often be much more difficult to 'embed' into a solution or product.

Privacy isn't just about how you protect your customer data, it's also about how your customers allocate rights to their data and how that information is shared and used among third parties.

The area that has been least frequently debated is the impact of 'trust' on the IoT relationship. Much more than simply 'brand trust' and reputation, IoT developers and tech firms will need to build an 'ecosystem' of trust and integrity with their users, partners, suppliers and customers in order to create new and more value-driven opportunities for customers. In some cases, trust can be achieved by leveraging the virtues of an already-trusted third party who protects the consumer or users.

We believe...

For security to be effective in IoT, it needs to be built into the technology and as close to the asset as possible: devices should have embedded security controls; software should have security embedded into the code. In fact, security should be a fail-safe control which means even when the technology is offline it is still secure. What we don't recommend is building 'open' devices or creating platforms where security is controlled centrally. The risks are too high.

Focus on security

Given the role that IoT devices are expected to play – managing everything from the temperature of the room to the speed of the car – it is surprising that the majority of IoT users have been slow to adopt the more traditional cyber security measures used in the market today.

In our survey, only around 40 percent of companies currently using IoT said they had already implemented measures such as improving firewall controls, enhancing identity management processes and running intrusion software.

Yet attacks are a reality. An example from the US in 2014 saw ICS-Cert (a branch of the US Department of Homeland Security focused on cyber threats) report a total of 245 incidents involving control systems (often the platform on which industrial IoT devices are integrated and controlled), of which 55 percent involved Advanced Persistent Threats (APT) – sophisticated attacks typically directed at high-value business targets. It was found that 42 percent of these targeted communication, water and transport infrastructure.[2]

As more devices shift online, threat actors will increase their efforts to overcome IoT security measures, whether for financial gain, political motivation, or to further exercise their skills and capabilities. And, as organisations start to rely more on IoT, these targets will become increasingly attractive.

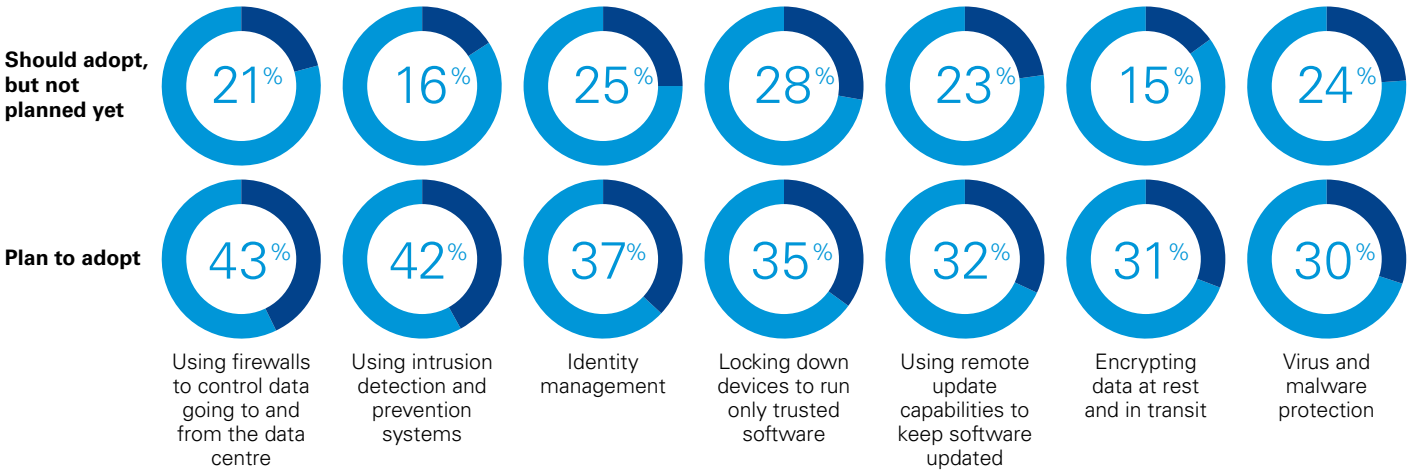
In order to deliver a safer and more secure IoT environment, tech companies and solution developers will need to take a lead role in making their devices and solutions as secure as possible.

Focus on privacy

As today's consumers increasingly recognise the value that their personal information represents to companies and service providers, they are becoming more comfortable with sharing personal information in return for improved services or lower prices.

However, underwriting this information-for-value covenant is a clear agreement on exactly what information can be

IoT users and solutions developers are hoping to leverage a broad basket of existing and potential technology solutions to respond to the risk of cyber-attack on their IoT solutions



Source: KPMG Cyber Security and IoT Survey

Of the following, which does your firm plan to adopt to tackle the security risks to IoT solutions?

2. https://ics-cert.us-cert.gov/monitors/ICS-MM201502

shared, who it can be shared with and for what purpose. A consumer with a wearable and connected heart monitor, for example, might allow this information to be shared with their healthcare providers, but would likely not want it to be shared with marketers or health insurers.

Organisations will increasingly negotiate with their users to gain permission to certain personal information in return for benefits. This is a unique opportunity to create and manage value-added services that both manages permissions and securely integrates and aggregates data.

Focus on trust

Much like personal information can be converted into value for consumers, trust can be converted into value for tech firms and IoT solution providers.

Gordon Archibald, Partner, Cyber, KPMG Australia, says trust must be a foundational element of any IoT development.

"A robust 'cyber security framework' requires collaboration and end engagement with all parties participating in the IoT ecosystem," he says. "Trust requires secure design so that we protect the ecosystem devices, communication channels and infrastructure that underpin the system – but also addressing regulatory demands, ensuring data privacy and building trust with customers."

Products and services from brands that enjoy a high level of customer trust not only have stronger relationships with customers, they also enjoy broader latitude to cross-sell services and products. Consider how certain technology companies have been able to parlay their existing brand and customer trust in one service area into market dominance in an entirely new one. Customer trust is key to long-term success in the IoT space.

Jan Zeilinga, Director, KPMG First Point Global says: "Things will only be secure, relevant and useful if the customer is in control and their digital identity becomes the trust anchor and primary control mechanism within the IoT ecosystem. Organisations that evolve their identity services to honour the preferences, privacy and security needs of things, people and information services will have a competitive edge."

We believe...

Some existing players will ultimately become the effective 'trust provider' within the ecosystems they operate in. The challenge will come when the 'trust provider' becomes the dominant brand rather than the device manufacturer or service provider thus, potentially, disintermediating the other players in the ecosystem.

Driving security, privacy and trust across the ecosystem

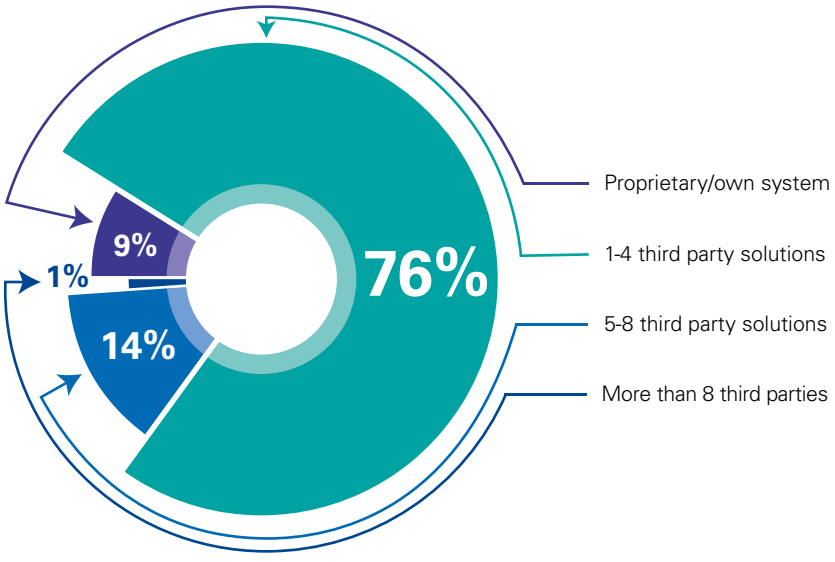
No one company can 'go it alone' in the IoT space; success will require organisations to partner, value chains to be created and ecosystems to flourish. Yet as IoT users start to bring more players, service providers and third party suppliers into their value chain, tech firms and IoT solution providers will face increasing pressure to demonstrate their security capabilities.

McLaren says business should only work with technology partners who have security 'built in from the ground up' in any IoT initiative.

"Businesses need to ensure they are looking at the full IoT ecosystem that they may be utilising – your security is only as strong as the weakest link. You may have a robust data storage approach – but a sensor that is easily hacked."

From device manufacturers and infrastructure service providers through to telco companies and data warehousing facilities, it will take a wide variety of players to create

The IoT ecosystem is growing and users increasingly understand that they need to rely on third parties and providers to develop a strong market proposition



Source: KPMG Cyber Security and IoT Survey
How many third parties are part of your IoT solution?

We believe...

The ecosystem will shift from a linear model with the customer at the end, to one where the customer is in the middle and ecosystem participants orbit around them.

In this environment, we expect to see traditional roles start to shift as players take on different roles in the ecosystem and overall value proposition.

However, our data suggests that few IoT users have fully considered how their new value chains will impact the overall security of their IoT solutions. In fact, 44 percent of respondents admitted that they had not yet considered how third party partners perceive security risks.

Conversely, smaller start-ups and those with low brand recognition in the market may find, by virtue of their partners in their ecosystem, that they can build up their customer trust fairly quickly.

the right ecosystem. Already, more than three-quarters of current IoT users say they use between one and four third parties to manage their IoT solutions; 15 percent say they use more than five third parties.

Ros Harvey, Managing Director, The Yield, says this concept of an ecosystem relates to the agriculture sector.

"The potential for IoT to drive benefit in the Australian agriculture sector is significant, but we need to have the right security measures in place," she says. "In agriculture trust relationships run deep. Growers need to have confidence that their data and their on-farm systems are secure. If that trust is compromised, adoption of IoT will suffer."

Cisco's Kevin Bloch raises the point that it is vital to be aware of the experience of IoT providers in your ecosystem.

"It has been said that half of the new IoT solutions over the next three years will be developed by companies less than three years old. It is probably unlikely that these companies will have expertise in security and privacy. This should be a big red flag for the industry," he says.

Assessing your third parties

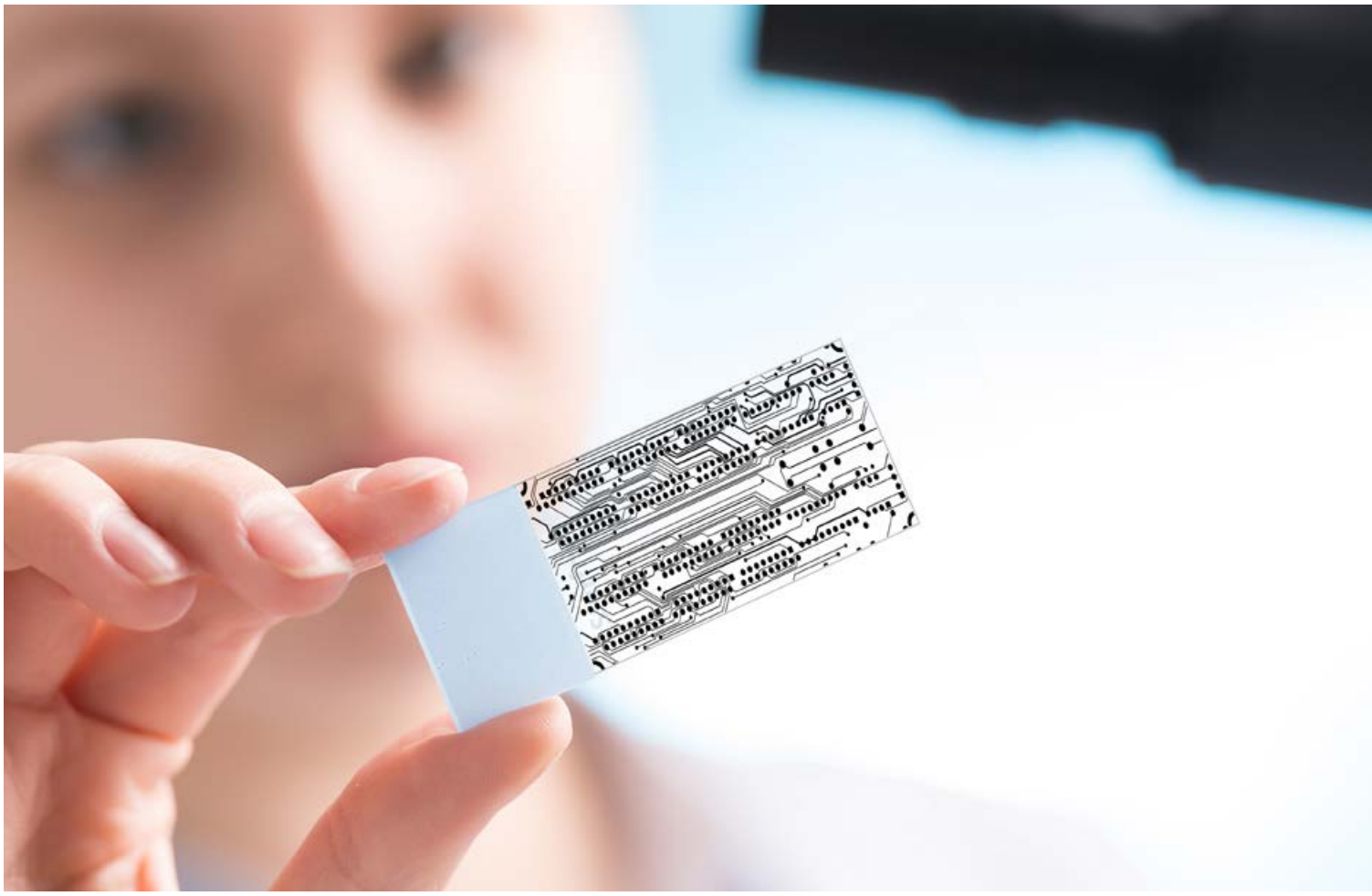
As the IoT market matures and adoption increases, we expect to see IoT users start to demand security, privacy and trust assurances that all of the suppliers in the ecosystem have policies and safeguards that align to those of the customer.

In some cases, organisations are introducing technology and tools, such as remote process monitoring to track supplier performance. Others are asking their suppliers to gain an accreditation or submit to audits to ensure alignment. Archibald says the IoT ecosystem includes numerous parties including manufacturers, software and tech companies, telecommunication operators, cloud providers and big data platforms, all with the potential to have security issues.

"An increasingly common approach is to use third party due diligence assessments and existing standards and attestation programs – such as the Service Organisation Control Type 2 Assurance Reporting (SOC2), which tests and reports on the design and operational effectiveness of an organisation's controls – to assess the security stance of third parties."

Archibald says that building Cyber Assurance and Cyber Resilience into the ecosystem is critical.

"Cyber Assurance is achieved through having confidence in controls (people, process, technology) deployed to protect the devices, systems, network and ultimately data. Cyber Confidence is partly achieved through 'Situational Awareness' and continuous controls-based monitoring which enables the ability to better protect and keep the ecosystem safe, but also identify and detect and respond to evolving threats."



5 key takeaways

1	**The IoT market is evolving.** The IoT sector is growing rapidly and will undergo several iterations of transformation. Similarly, concerns related to security, privacy and trust will also evolve and transform as the market changes. Security strategies should be broad-based to anticipate and respond to potential disruptions that could impact current market positions.
2	**The IoT ecosystem plays a critical role in securing IoT.** Businesses should carefully evaluate their third party suppliers, identify qualified partners, and invest in integrating security, privacy and trust across the ecosystem. Business should consider different approaches to building the capabilities they require within the ecosystem, including whether they can buy, build, partner, invest, or create an alliance to achieve their goals.
3	**Security must be built-in from the ground up with the customer in mind.** Consumers, businesses and government will expect security to be built into the system; technology architects should follow an 'always-on' principle that provides high levels of control with appropriate fail-safes. Given the scale and velocity of IoT growth, security vulnerabilities can become large liabilities to the company.
4	**Look for opportunities to drive value from security.** Security architects should reconsider the security models to identify potential to enhance the value of security. Consider, for example, using premium concepts of security, privacy, and trust to differentiate the product. Security for IoT is not just about protecting valuable data, it's also about finding opportunities to monetise the intelligence.
5	**Engage in industry and regulatory groups to accelerate the normalisation and standardisation of IoT.** Collaboration will reduce ambiguity and accelerate a company's ability to launch products and services within a sustainable business ecosystem. Regulators will also need to participate in industry discussion in order to protect market and consumer interests. Technology companies should be proactive to help regulators to support IoT.

Contact us

For further information about this publication and on the services offered by KPMG's Technology, Media & Telecommunications practice, please contact:

Chris McLaren
Partner
National Sector Leader
Technology, Media
& Telecommunications
T: +61 2 9335 8507
E: chrismclaren@kpmg.com.au

Gordon Archibald
Partner
Cyber
T: +61 2 9346 5530
E: garchibald@kpmg.com.au

kpmg.com.au

March 2016. QLDN13805LOBS.