Security and the IoT ecosystem

KPMG International

kpmg.com

Foreword

When it comes to the Internet of Things (IoT), you can believe the hype. In fact, IoT will likely be even bigger than most people think. 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.

It seems obvious that IoT will bring massive growth to those tech companies and IoT developers that are able to 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.

Indeed, as 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.

We believe that 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 catalyze the debate and extend the body of knowledge on IoT security. In the following pages, we start to explore the security, privacy and trust challenges influencing the IoT space and delve into some of the opportunities and models emerging in the market today. Based on a recent global survey of 100 IoT 'user organizations' and supported by one-on-one interviews with industry leaders, academic and KPMG's own IoT professionals, this report hones in on IoT security, privacy and trust, providing practical and actionable advice for all players in the emerging ecosystem.

Over the coming year, KPMG International 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.

Gary Matuszak

Global Chair
Technology, Media & Telecommunications

Greg Bell

Principal and Services Leader, KPMG Cyber
KPMG in the US

Danny Le

Partner
KPMG in the US

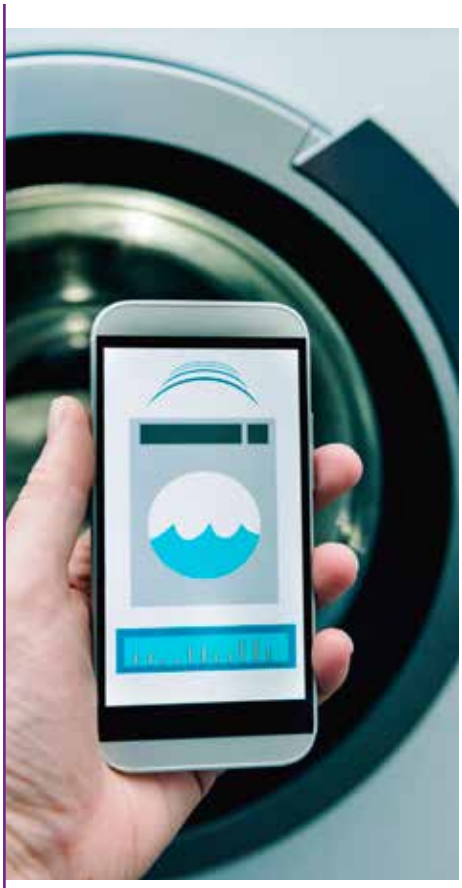
The Internet of Things (IoT)

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

02

Cyber security becomes a ‘must have’



06

Looking for standards

10

Focus on security, privacy and trust

16

Driving security, privacy and trust across the ecosystem

Cyber security becomes a 'must have'

92%

of IoT users are concerned about cyber security

Source: KPMG Cyber Security and IoT Survey

Business leaders may recognize the potential advantages that IoT can offer. But they are also deeply worried about the risks; the majority admit that they don't fully understand the cyber security threats that IoT brings.

But while IoT customers may not be willing to pay extra for security, recent security breaches in consumer data and systems suggest that they will lose confidence and may even avoid solutions 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 capitalize on the massive growth potential of this emerging field.

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. But the reality is that history is littered with products and ideas that placed speed-to-market over substance and, as such, quickly lost their advantage to other – less nimble but more robust – competitors. Simply put,

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

This reality is already being borne out. Recent revelations about security vulnerabilities in a number of newer-model automobiles have forced some major manufacturers to conduct massive recalls. Over the summer, the media was abuzz with news of hackers 'hijacking' cars through badly-secured software systems.

Taking the threat seriously

Many organizations are now thinking more clearly about how they might improve IoT security. "At Intel, we believe that integrating security into the platform and into the silicon is critical to helping drive IoT's adoption and scalability. Integrating security at the onset is key to establishing trust for IoT solutions," noted Bridget Karlin, Managing Director, Internet of Things Group Intel. "We've got some great IoT offerings coming onto the market that

> "Our company's understanding of IoT cybersecurity risks is limited, so it has become a top priority."
> – CEO of a European-based IoT user organization

IoT: Rapid growth, massive potential

No one doubts that the Internet of Things (IoT) represents a massive opportunity for businesses, consumers and tech companies. Most organizations are only 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, we believe that as consumers get more and more familiar with the benefits that IoT can deliver – smart appliances, automated vehicles, wearable devices and much more – key concerns around security, privacy and trust are likely to grow.

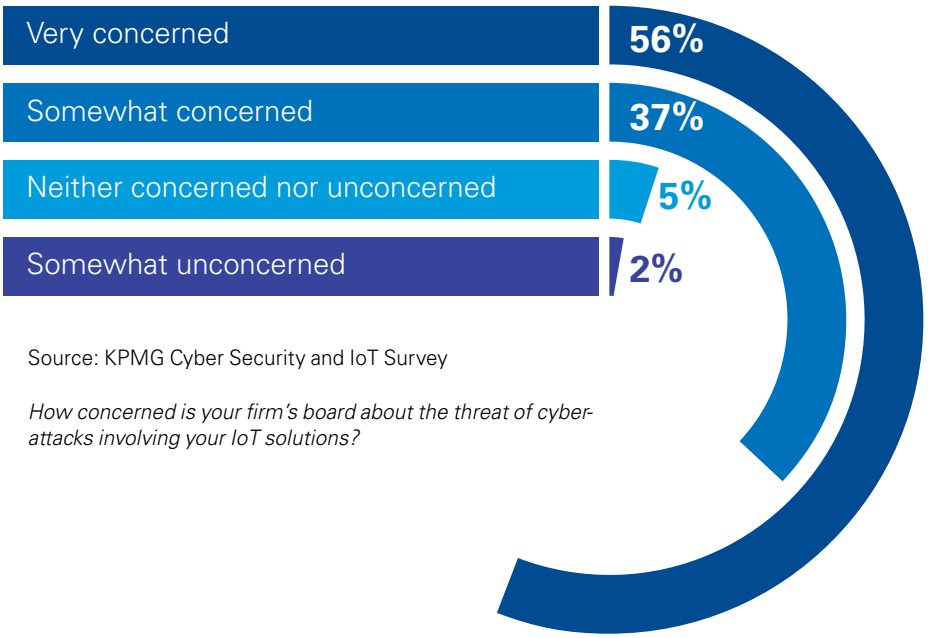
1 Worldwide and Regional Internet of Things 2014–2020 Forecast, IDC Research, 2014

enable secure and scalable end to end IoT solutions using our Intel IoT Platform reference architectures and portfolio of products that provide hardware and software enforced integrity and data privacy."

For their part, IoT users are certainly concerned about the potential impact of a cybersecurity breach within their IoT solutions. More than half – 56 percent – of respondents in our survey said that their board was 'very concerned' about the threat of cyber-attack. More than a third said their board was 'somewhat concerned'.

As one Asia-Pacific-based Chief Risk Officer told us, "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 the device, improved security in IoT can also provide significant advantages. Our experience suggests that a strong and robust cyber security stance, commonly accepted standards and strong actions towards earning consumer trust will be key to ensuring long-term advantage and, ultimately, supporting growth.

"Key concepts around IoT security, privacy and trust must be front-and-center for tech firms and IoT solutions developers," noted Danny Le, Partner, KPMG in the US. "The 'upside' to cyber security is coming. In fact, before too long we expect to see organizations turn cyber security prowess into real revenue opportunities by, for example, monetizing identity and usage patterns. But this, too, will come with its own inherent risks and rewards."

Some companies are already monetizing their customers' personal data. Telecoms companies, for example, are using customer geolocation data (with permission) to tailor offerings from 3rd party vendors such as insurers and retailers; car 'communities' are being created around customer driving patterns. Yet continued expansion of these models will require that all those involved in the ecosystem are able to keep that data private, secure and confidential.

Those tech companies and IoT solutions developers that take a disciplined approach, investing the appropriate time and resources to integrate security, privacy and trust concepts into their IoT solutions will – ultimately – win out over those that eschew discipline in order to be first to market.

> "Security really needs to be designed into IoT solutions right at the start. You need to think about it at the hardware level, the firmware level, the software level and the service level. And you need to continuously monitor it and stay ahead of the threat."
>
> —Florence Hudson, Senior Vice President and Chief Innovation Officer Internet2 (formerly with IBM)

Looking for standards

Characterized by massive growth, wildfire adoption and rapidly emerging use cases, IoT is a virtual 'Wild West' with few rules, little regulatory oversight and masses of pioneers competing to strike their fortune. The industry, regulators and users will need to come together to form generally-accepted standards and ecosystems.

In part to improve the interoperability of IoT solutions and in part to help define the minimum expected security standards, many organizations now believe that the development of industry standards will be the single 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 tech firms – both large and small – have started to create consortiums of like-minded organizations to help focus on creating and commercializing new standards. New consortiums and standards are being announced every few months, leading to tight competition and significant uncertainty for players in the market.

Google's Nest product, for example, has partnered with companies such as Samsung Electronics, ARM Holdings, Freescale Semiconductor and Silicon Labs to develop their 'Thread' networking protocol aimed at standardizing IoT communications in the home. At the same time, Intel has partnered with Cisco, AT&T, GE and IBM to create standards specifically for industrial IoT use. Cisco is also part of the AllSeen Alliance created by Qualcomm, alongside heavyweights such as Microsoft, LG and HTC to create an interoperable peer connectivity and communications framework. And in August 2015, the Online Trust Alliance was launched as a collaborative effort that includes firms such as Microsoft, Symantec, Target and ADT who plan to offer guidelines for IoT manufacturers, developers and retailers with a focus on consumer IoT devices.

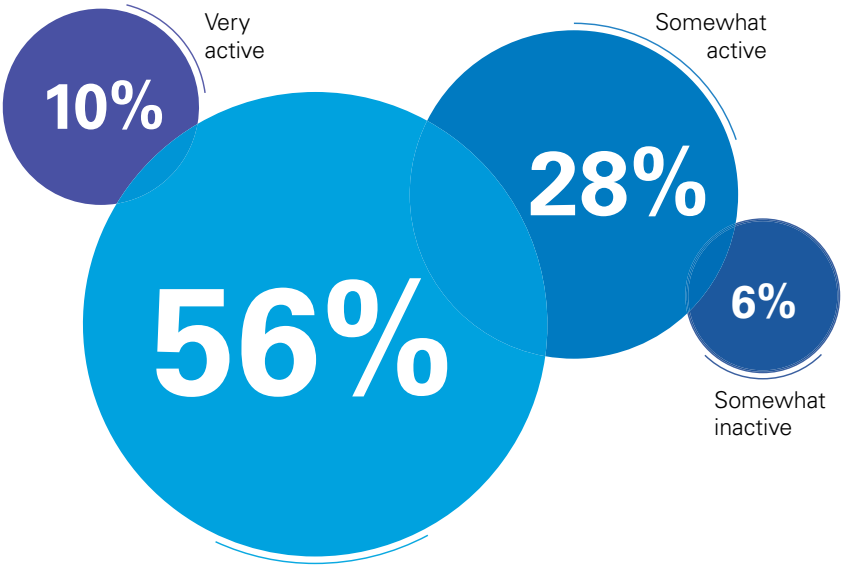
> “Companies need to stop thinking about regulation as a cost to manage and instead start taking a longer-term view. They need to be asking themselves how they can influence the development of regulation and how that impacts the emergence of the market and the success of the business.”
>
> —Dr. Michael Geist, Canada Research Chair, Internet and E-commerce Law, University of Ottawa

"This industry is very fragmented, with lots of standard and quasi-standard bodies addressing similar issues – thus aligning the industry around the same approach and standard requires a broad alignment and participation," noted Maciej Kranz, VP, Strategic Innovations, at Cisco.

Collaboration or competition?

Given the pervasiveness of IoT and the sensitivity of the systems and data, nobody active in the sector doubts the need for clear IoT regulation and standards. As Chris Wiegand, CEO of Jibestream notes, "It's the industry that

Most IoT user organizations are taking a laid back approach to driving the IoT debate



Source: 2015 KPMG Cyber Security and IoT Survey

Within your industry, how active a role has your firm taken in starting a dialogue about the IoT?

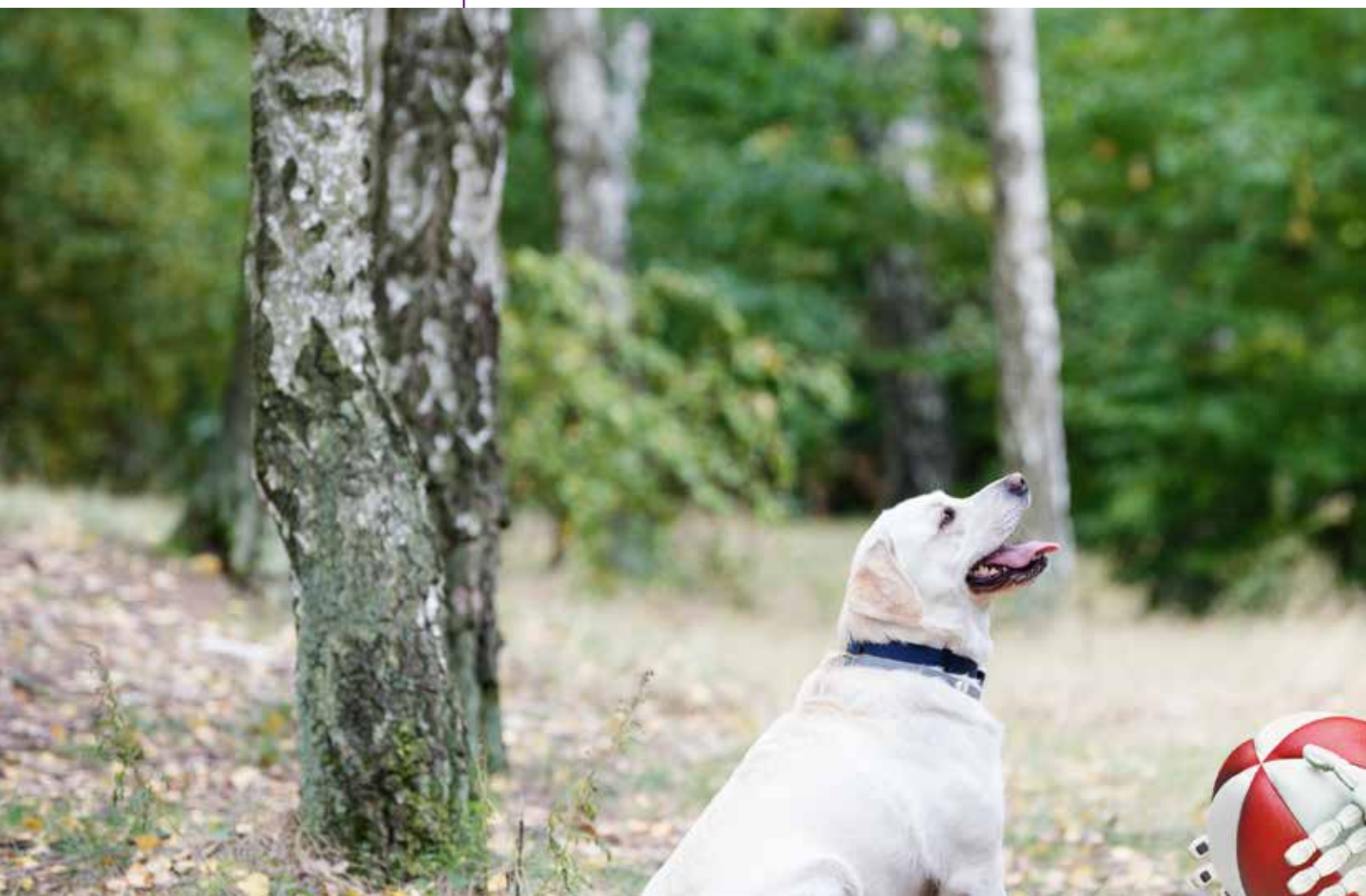
is really developing the Internet of Things and we need to ensure that we do it right and not in a way that exposes it to misuse or abuse."

However, there are some concerns among players that competition over standards will only harm the sector. As Internet2's Florence Hudson notes, "There is a splintering happening where everyone is trying to create consortiums, but everybody is also trying to win. So what I'm hoping is that we can create an eco-system across the industry at every point to develop these themes of security and privacy, and then use these consortiums as channels to execute it."

Increased regulatory oversight and guidance will also help 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.

Those in highly regulated industries – financial services, healthcare and utilities, for example – have particular reason to be concerned.

"Regulators often have trouble catching up with new innovations and – until they do – often take a dim view of change within their sector; it is not surprising that many US healthcare organizations are looking to the FDA to tell them which wearable devices will be accepted within the US health sector," added Greg Bell, Principal and Services Leader, KPMG Cyber. "Regulation is a double edged sword – on the one side it requires organizations to invest in compliance and reporting but, at the same time, it also clarifies what will and won't be accepted, allowing organizations to move ahead with their investments and planning."



In some sectors, however, the lack of regulation may be slowing the adoption of IoT solutions. Many Tesla drivers, for example, now have access to an 'auto-pilot' feature which promises to reduce accidents and improve safety, which when matured to autonomous driving vehicles may even reduce accidents. But – to date – road regulators have been unwilling to allow the feature to be used on public roads, thereby severely limiting the competitive advantage gained through this novel technology.

More to do

Our experience suggests that few technology companies and IoT solutions developers are actively working towards creating standards. Fewer still are engaging with regulators to understand – and to inform – the direction of future regulatory travel.

"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," noted Malcolm Marshall, Global Leader, Cyber Security. "This is no 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."

However, as Cisco's Maciej Kranz reiterates, "There's at least 10 to 15 different standard bodies that are thinking about each aspect of security, privacy and trust in IoT, and it's important that we consolidate these efforts and take a holistic approach versus each of the industries coming up with their best practices and standards."

Focus on security, privacy and trust

We believe that 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.

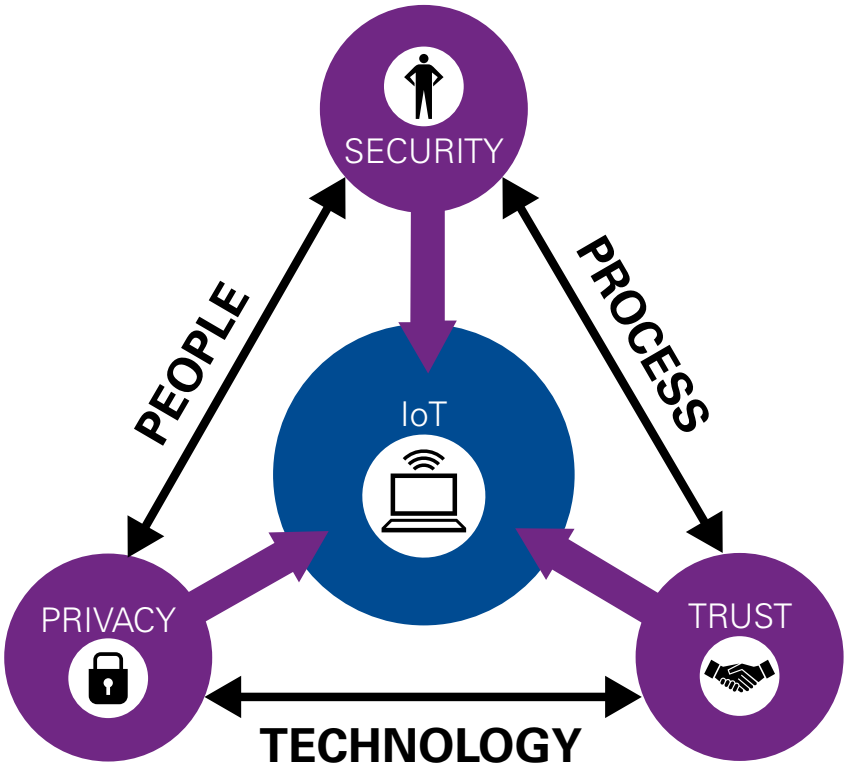
While the topic of cyber security certainly seems to be front and center for both IoT users and developers, our experience suggests that most are taking a rather narrow view of their obligations. We believe that a robust 'cyber security' approach focuses not only on protecting the devices and infrastructure 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?

Often confused as a single concept, the reality is that successful IoT solutions, products and innovations will require tech firms and solutions developers to think more specifically about three key concepts that enable a valuable user experience: security, privacy and trust.

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

Privacy, on the other hand, relates to confidentiality and data control and – as such – 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 3rd parties.

The area that (to date) has been least frequently debated has been 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 3rd 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 "off-line" it is still secure. What we don't recommend is building 'open' devices or creating platforms where security is controlled centrally. The risks are just too high.

> "They're going to try to hack everything," warns Florence Hudson of IBM. "I am most worried about security in healthcare, in cars and moving vehicles and in critical infrastructure."

Focus on security

Given the role that IoT devices are expected to play in the new world of tomorrow – 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 many of the more traditional cyber security measures used in the market today.

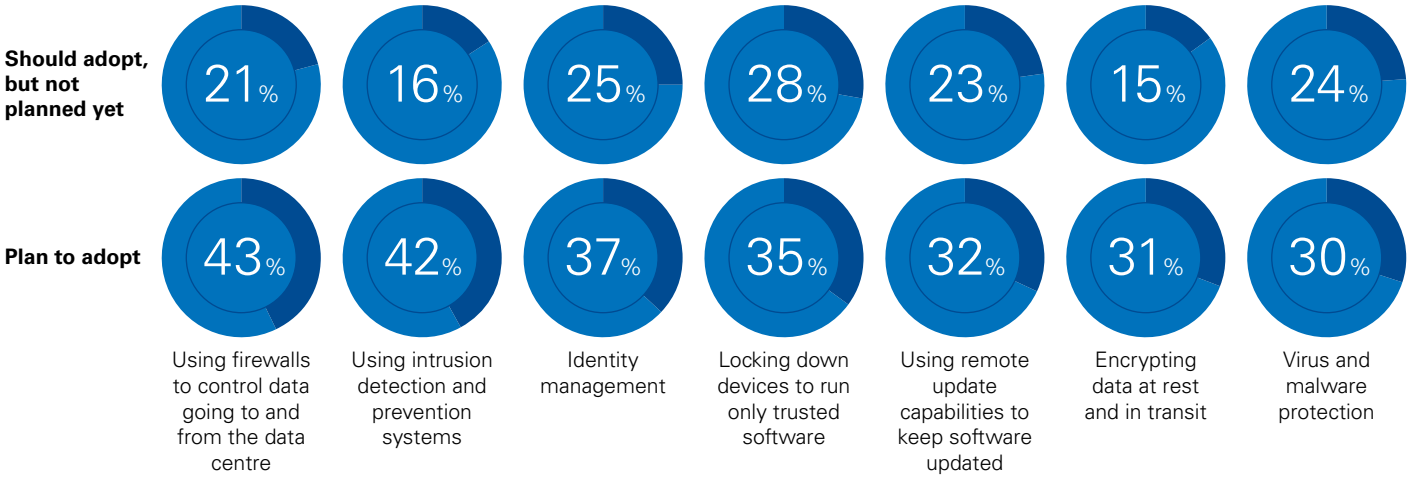
In our survey, only around 40 percent of companies currently using IoT said they had already implemented measures such as improving firewall controls, enhancing identify management processes and running intrusion software.

Yet attacks are already a reality. In 2014, ICS-Cert (a branch of the US Department of Homeland Security focused on cyber threats) reported 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; 42 percent of these targeted communication, water and transport infrastructure[2].

It seems clear that – as more and more devices shift online – threat actors will increase their efforts to overcome IoT security measures, whether for financial gain, political motivation, or simply to further exercise their skills and capabilities. And, as organizations start to rely more and more on IoT data, these targets will become increasingly attractive to these committed threat actors.

In order to deliver a safer and more secure IoT environment, tech companies and solutions developers will need to take a lead role in making their devices and solutions as secure as possible. "Security really needs to be carefully considered right at the design phase and then continuously tested and updated throughout the development process," noted Gary Matuszak, Global Chair, Technology, Media & Telecommunications. "Those that are able to add in 'after-market' updates and upgrades will not only deliver more value to their customers, they will also help maintain their own reputations in the market."

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

Focus on privacy

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

However, underwriting this information-for-value covenant is a clear agreement on exactly what information can be shared, who it can be shared with and for what purpose. A consumer with a wearable and connected heart monitor, for example, would expect this information to be shared with their healthcare providers, but would likely not want it to be shared with marketers or health insurance plans.

Rather than just being a risk, however, the debate about privacy is quickly evolving to one of opportunity. Simply put, consumers are recognizing the value that their personal information offers – not only their transaction records, but also their behavioral data and their metadata – and are already essentially 'trading' their information to companies for better service, lower costs or promotions. This, in turn, is leading to new opportunities and potential value for IoT organizations.

"Personal information is quickly becoming a new form of currency for consumers and, in the right circumstances and for the right pay-off, IoT users will be happy to share their data," noted Henry Shek, Partner, KPMG in China. "But that means that IoT solutions providers, their corporate customers and everyone else in the IoT value chain will need to be very clear about what data can be shared and with whom."

We believe…

Organizations will start to negotiate with their users to gain permission to certain personal information in return for clear benefits. As such, tech companies and IoT developers have a unique opportunity to create and manage value-added services that both manages permissions and securely integrates and aggregates data.

We believe…

IoT will lead to greater integration between products and services – integrating traffic-aware mapping services into cars or developing payment applications for phones, for example – as organizations focus on providing a more complete and seamless quality experience to their end-users.

> "What's on most people's minds right now is keeping customer trust and issues surrounding privacy, security and integrity of data."
>
> —Danny Le, Partner, KPMG in the US

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. There is a mountain of literature that demonstrates the irrefutable connection between 'brand trust', customer experience and sales.

Products and services from brands that enjoy a high level of customer trust not only tend to have stronger 'relationships' with customers, they also enjoy broader latitude to cross-sell services and products. Consider, for example, 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 – such as mobile payments – where, arguably, they had no prior experience or footprint at all. Clearly, customer trust is key to long-term success in the IoT space.

"In part, trust is based on your ability to maintain the security of the system and your ability to protect customer information, but it also must include considerations related to your brand image, the way you communicate with consumers and how you respond to unintended security or privacy breaches," added Richard Marriott, Senior Manager, Cyber Security KPMG in the UK. "You can't just assume that if you secure it, trust will come. You have to really work at building it."

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.

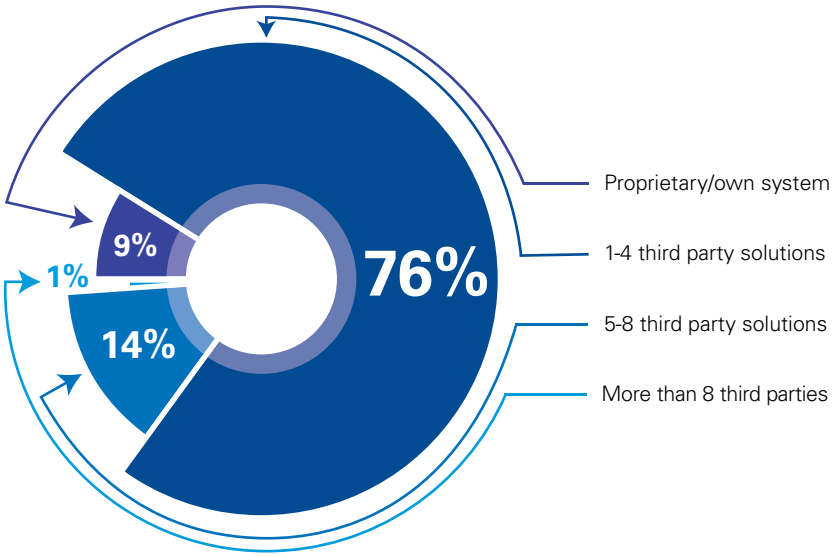
Driving security, privacy and trust across the ecosystem

No one company can 'go it alone' in the IoT space; success will require organizations to partner, value chains to be created and ecosystems to flourish. Yet as IoT users start to bring more players, service providers and 3rd party suppliers into their value chain, tech firms and IoT solutions providers will face increasing pressure to demonstrate their security capabilities.

From device manufacturers and infrastructure service providers through to telco companies and data warehousing facilities, it will take a wide variety of players to come together to create the right ecosystem for IoT. Already, more than three-quarters of current IoT users say they use between one and four 3rd parties to manage their IoT solutions; 15 percent say they use more than five 3rd parties.

"The reality is that none of the companies can do it alone. At Cisco, we're developing a large number of partnerships, both horizontal and vertical, to develop and deliver the platform capabilities and solutions," noted Cisco's Maciej Kranz.

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

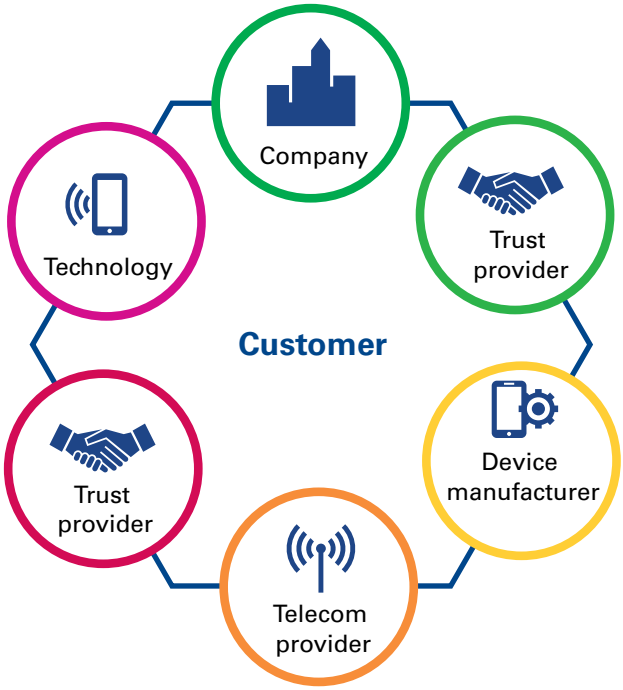
How many third parties are part of your IoT solution?

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 start to take on different roles in the ecosystem and overall value proposition.

Then technology ecosystem used to be linear … .

In today's IoT ecosystem, players 'orbit' around the customer



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 our respondents admitted that they had not yet considered the way in which 3rd party partners perceive security risks.

"Cyber-attack on devices is a real risk right now and we have to mitigate that risk by choosing vendors that offer some level of management or security, and staying away from others that are kind of treating the whole IoT world as the Wild West right now," said Chris Wiegand of Jibestream.

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

Assessing your 3rd parties

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

According to one North American CIO, "We have appointed an accredited evaluation party to assess the security standards of our external partners as an added responsibility and they have agreed to the same for a reasonable amount which fit our budget."

An increasingly common approach is to use 3rd party due diligence assessments and existing standards and attestation programs – such as the Service Organization Control Type 2 Assurance Reporting (SOC2), which tests and reports on the design and operational effectiveness of an organization's controls – to assess the security stance of 3rd parties. SOC 2 is based on five key 'trust service principles': security, availability, processing integrity, confidentiality and privacy. For example, in the US healthcare sector, SOC 2 is increasingly being used to ensure 3rd parties are not only maintaining a high level of security, privacy and trust, but also that they are compliant with key data security regulations such as HIPAA.

We believe…

All of the participants in the ecosystem must have a responsibility to protect the security, privacy and trust of the solution for the 'handshake' to work in order to protect the end-user.

5 key takeaways

1. **The IoT market is evolving.** The IoT sector is growing rapidly and will likely undergo several iterations of transformation. Similarly, concerns related to security, privacy and trust will also evolve and transform as the market changes. As such, security strategies should be broad-based to anticipate and respond to potential disruptions that could impact current market positions.

2. **The IoT eco-system plays a critical role in securing IoT.** Businesses should carefully evaluate their 3rd 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 and business partners 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 monetize the intelligence.

5. **Engage in industry and regulatory groups to accelerate the normalization and standardization of IoT.** Collaboration will reduce ambiguity and accelerate a company's ability to launch products and services within a sustainable business ecosystem. At the same time, 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:

Gary Matuszak
Global Chair
Technology, Media & Telecommunications
T: +1 408 367 4757
E: gmatuszak@kpmg.com

Greg Bell
Principal and Services Leader, KPMG Cyber
KPMG in the US
T: +1 404 222 7197
E: rgregbell@kpmg.com

Danny Le
Partner
KPMG in the US
T: +1 213 430 2139
E: dqle@kpmg.com

Acknowledgments

We would like to thank the following people for their valuable contribution to this study:

All survey respondents, Florence Hudson, Michael Geist, Bridget Karlin, Maciej Kranz, Chris Wiegand and our external writer Peter Schram.

KPMG's firms' partners and principals who provided their insight, including Malcolm Marshall, Richard Marriott, and Henry Shek.

The KPMG International project team: Sunitha Shivakumar, Alise Barnes, and Carolyn Forest.

kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Designed by Evalueserve.

Publication name: Security and the IoT ecosystem

Publication number: 132631-G

Publication date: December 2015