KPMG

The internet – everywhere, in everything

Key insights from the Everything IoT Data Security Forum

Sydney, March 2016

kpmg.com.au

The Internet of Things (IoT) is what makes everything from streetlights and airports to fridges and pacemakers “smart”. Built on cloud computing, IoT uses networks of data-gathering sensors and instantaneous connections to get machines talking to each other. As it transforms more areas of human life, we need to be able to trust that IoT is doing its job correctly, won’t malfunction and is secure.

Everything IoT’s latest Australian forum addressed these issues on 9th March, 2016 at The University of Technology, Sydney – the first of four IoT events to be held by the organisation this year.

An expert panel discussion, Enabling IoT adoption in Australia, was moderated by Eitan Bienstock, Founder, Everything IoT, and Director of Global Growth, ATP Innovations. In this report, we pinpoint the essential takeaways from the event.

An alarming lack of security awareness

In 2015, Wired Magazine conducted a fascinating Jeep Cherokee experiment. While a journalist drove a Jeep through a desert, two cyber security experts managed to remotely change the music on its sound system, start the windshield wipers and finally take control of the accelerator and brake. However after a product recall, Fiat Chrysler reported that its Jeep Cherokee computer systems were "defect free".

Bienstock says the main lesson was that the manufacturer did not recognise hack-ability as a problem.

"It is symptomatic of the alarming lack of awareness among consumers and corporations on the risks associated with IoT interconnectivity," he says.

Israel's leading cyber security expert, Professor Isaac Ben-Israel, outlines where this perspective comes from.

"For the past 50 years, information security has looked at how we protect data on closed networks," he says. "And that is how a lot of corporations and governments still think. But IoT runs on open software to connect devices, businesses and things in very complex ways. It's a totally different ball game."

In addition to the challenge of increasing the awareness of the security risks both for the industry and consumers, Bienstock has pointed out two additional challenges facing IoT data security:

- After 25 years of figuring out how to protect privacy in corporate systems and public internet, we now need in just a few years to figure out how to protect physical risks from self-driving cars through nuclear reactors to pacemakers.
- Data security is a foundational enabler for the implementation of IoT and therefore is a crucial element to determine the speed by which the expected trillion dollars in benefits that IoT implemention has the potential to provide will be achieved.

> “
>
> IoT runs on open software to connect devices, businesses and things in very complex ways. It's a totally different ball game.

Unlearnt lessons from 2010

In 2010, malware attacked and destroyed Iran's uranium enriching centrifuges. Not directly, but by changing the software in the rotation controllers of the centrifuges. Ben-Israel argues that there are three lessons from this attack that are still not widely acknowledged today:

1. Cyber security is not only about protecting data. It is also about protecting "things", and preventing physical damage.
2. Many still believe security is about firewalls and protection systems on computers. The attack on Iran did not come through the internet. The facility was not connected to any external nor internal networks.

   Every computer has a way to be updated – to inject information inside – transistor chips. An isolated computer doesn't exist.
3. The Iranian facility had no 'computers' but only 'controllers' that are really computer chips, and therefore can be hacked too.

"When people start to think about IoT, they think smart gadgets, smart buildings and smart cities. All this smartness comes from the chips in the computers," he says.

"Today, we can computerise any device in our home or office and interconnect them without human intervention. My phone calendar links to an app to check my schedule and the traffic reports for my route, then sets my alarm for the right time. Transistor chips are now so small that we are putting them everywhere, including inside our bodies."

Ben-Israel points out that the US Defence Force investigated their entire chip supply and found that 80 percent were made in China.

"With transistors already down to 140 silicon atoms in size, it is almost impossible to know what has been embedded in any device."

How Israel protects against IoT hacks

According to Moore's Law, we see two generations of a smart phone or computer every three years. So a traditional 5 year security plan isn't going to work. Ben-Israel argues that a living ecosystem is needed. An IoT system that keeps up with changes, generates solutions by itself and operates 24/7.

The insurance headache

Antonio Derossi, Propeller Venture Capital, Managing Partner, Insurance, explains that IoT is changing insurance in two dramatic ways:

1. Traditional risks are decreasing. There is a lot of information that was not available before. It is much more precise to underwrite a person when the insurer has their biological data. It's the same for properties, with information coming from connected devices, automated appliances, smoke detectors etc. Underwriting risk is much more accurate with IoT.

   There is also better loss prevention. The driverless car or automatically controlled plane is likely to make fewer incorrect decisions that lead to accidents. Drones looking at roofs can reduce property damages.

2. There are new cyber risks and new ownership of risk. If there is a malfunction or someone hacks an IoT device, who is liable? In the case of a driverless car, is it the person nearest the steering wheel or the producer of the vehicle or the software? Until liability is agreed, many products cannot go to market.

Derossi explains that until very recently, the internet was all about exchanges of information and retail – Amazon and eBay.

"Now, it's rapidly becoming a hub for healthcare, manufacturers' services, electronics and media entertainment," he says. "The immense quantity of open software that runs all of this connectivity is not sufficiently tested for insurance and risk assessment purposes. There are no precedents to base our assumptions on."

Derossi believes the outcome will see less liability on the personal side and more on the professional side. However, the complexity of professional liability (manufacturers vs. software designers vs. maintenance companies etc.) and the appearance of new cyber risks must be compensated by the better management of risk.

"Essentially, this means insurance moves from liability for a one-off accident to liability around cyber security. Companies are not on guard to properly protect the data on their systems. It is a whole set of new liabilities they will be exposed to," he says.

> "
>
> The immense quantity of open software that runs all of this connectivity is not sufficiently tested for insurance and risk assessment purposes.

"But it's just a toothbrush." The legacy of Australia's "she'll be right" attitude.

Australia is developing IoT products every day, and Simon Blyth, Founder and CEO of LX Group pointed out that there are two attitudes to security: One says: "IoT security is really important to me. Let's get it right." The other says: "It's just a … toothbrush, blender, fire alarm etc." The problem is that commercial reality means producers want to cut corners. There is not an understanding of what can happen when devices are connected.

Chris McLaren, National Sector Leader, Technology, Media & Telecommunications at KPMG says that from a corporate perspective, the attitude to security is a cultural issue.

"The board has to believe it's critical," he says. "They've got to be propagating it down. In a recent survey of the top 10 priorities for boards this year, number three was cyber security. Every board has to define its attitude to risk, security and innovation."

> In a recent survey of the top 10 priorities for boards this year, number three was cyber security.

McLaren adds that generally, Australian corporations and government have a limited awareness of IoT in terms of opportunities, the risks of poor adoption and the potential disruptions to their business from those who are adopting it well.

"If awareness is out there, it will be at the personal level of a Fitbit or smart watch. But they don't think about what it might mean for them as an insurer, banker or farmer."

McLaren explains that organisations like IoT Alliance Australia are needed to raise awareness of the positive and negative risks of IoT and build an ecosystem around it.

"There are obviously great opportunities to be IoT consumers, but there's also a great opportunity to create and commercialise the technology, which Australia hasn't historically done that well in."

Helping business assess IoT cost, risk and growth potential

According to McLaren, Board and Chief Risk Officers tend to think of things through three lenses: cost, risk and growth.

"Organisations like the IoT Alliance Australia can help broker interaction between start-ups, the IoT technical ecosystem, business and government. It's a journey, and Australia is probably two or three years behind most other countries in this."

He emphasises the need for government leadership and involvement in fostering IoT and points to the United Kingdom as an example.

"The government there is successfully fostering IoT, particularly in the smart city space. And they are working hand-in-hand with the technology ecosystem to get the balance right – to drive innovation, to balance out where rules need to be built and standards created."

He adds that this is why the IoT Alliance Australia is putting together a position paper to go to government.

"It puts forward the technology community's views on what the government needs to be doing and thinking about regarding IoT so we don't miss this wave."

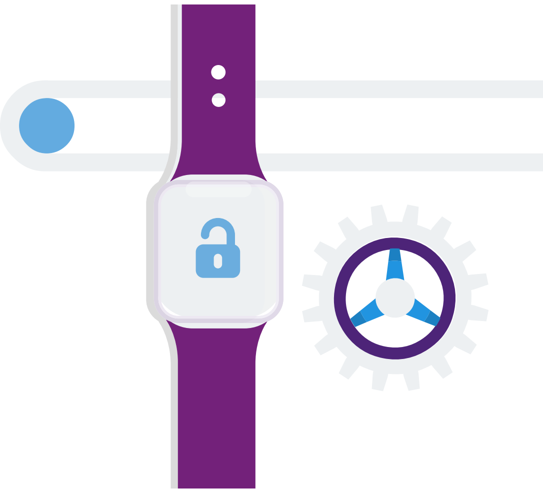
Michelle Price, Senior Advisor, Domestic Cyber Policy, Prime Minister and Cabinet, adds that while Australia has survived on the legacy of a "she'll be right" culture, things are changing.

"If Australia wants to benefit from, rather than export its capabilities, we have to get a lot smarter about this," she says.

Price admits that Australia does have a history of solving policy problems by letting them run through a little.

"That is partly about gaining experience and seeing how new situations play out. At a government level, we know IoT is here to stay. It is our new world. However, we need to examine the ripple effect of any IoT policy on other factors driving economic growth – like the Cloud."

> "
>
> If Australia wants to benefit from, rather than export its capabilities, we have to get a lot smarter about this.

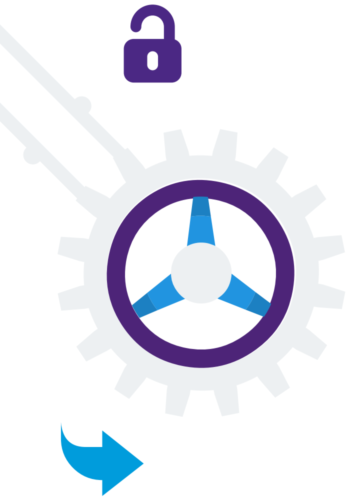


Looking into the future of IoT

Cameron Yuill, Founder and Managing Partner of Propeller Venture Capital, puts things in perspective: "If you think back 20 years or so, it was all about 'the internet'," he says. "Then 'mobile' came along and it was divided into sectors and regions by investors and producers. IoT is the same. IoT is at the top of its hype cycle and lots of VCs are raising capital in it right now. However, it will break down into obvious sectors like agriculture and manufacturing. There will be very specific niches too, including cyber security."

Ben-Israel reminds us that every 1.5 years we put twice the number of transistors on a chip.

"So in less than 10 years we will reach transistors of one silicon atom in size. That will be the end of the story for transistor miniaturisation. From then on, we will need another technology."



IoT and quantum computing

That new technology is quantum computing. The prototypes are only at a handful of universities and not commercialised. However, Ben-Israel says that generally speaking, it is agreed that commercially viable quantum computers will exist 15 to 25 years from now.

He points out that quantum computers of 100 qbits will be 1030 times faster than the best transistor technology today.

"One billion of a billion billions is only 1,000th of 1030. What we will do with quantum computers is immeasurable and inconceivable.

"Anyone can have what was considered a super computer some years ago. Quantum computers will be no different'.

"At the beginning, perhaps only certain governments will have them for intelligence purposes. But once it is cheap and small enough, no one will resist the temptation to commercialise it. Think about satellites."

He points out that quantum computer technology is related to quantum encryption.

"There are ways to encrypt information using quantum devices that are in principle unbreakable."

Preparing to ride the IoT wave securely

Ben-Israel emphasises that Australia cannot rely on the government to create an IoT ecosystem. "Governments should only encourage and not interfere too much, like we did in Israel", he said.

"We took the Israeli hi-tech ecosystem and shifted it a few degrees towards cyber security. It actually gave us an opportunity to grow our high-tech industries. But to do it, you need to include all the different areas of technology – start ups, corporations, government and academic institutions. But you need the right people working in your ecosystem."

He explains that Israel set up five university cyber security research centres.

"Cyber security problems usually have technology solutions but the problems are never technological. They are human. Our research teams are 70 percent science and 30 percent soft subjects like psychology, law, business, and political science."

Israel is the only country to date where cyber security is a high school subject.

"It is really mathematics and computer language – but much sexier for kids, which means more of them study it. That helps ensure our universities get prepared researchers."

Ben-Israel shows the statistics that support his claims: In 2014, Israel's share of the global cyber security market had increased to around 8 percent (400 percent growth in 4-5 years). In terms of investments in cyber Research and Development (R&D), Israel got some 15 percent of the global market. Overall, Israel leads the world in R&D per capita (4.5 percent of the GDP). In other words, the investment into their IoT and cyber security ecosystem is already paying off.

Forum panel speakers:

Professor Isaac Ben-Israel. Major General (retired), Headed Israel's National Cyber Policy Task Force, Chair of Israel Space Agency and Israel national Council for R&D and Head of the Blavatnik Interdisciplinary Cyber Research Centre and of the Security Studies Program, Tel Aviv University.

Antonio Derossi. Propeller Venture Capital, Managing Partner, Insurance.

Cameron Yuill. Founder and Managing Partner of Propeller Venture Capital.

Chris McLaren. National Sector Leader, Technology, Media and Telecommunications, KPMG Australia.

Michelle Price. Senior Advisor, Domestic Cyber Policy, Department of Prime Minister and Cabinet.

Eitan Beinstock. Founder of Everything IoT Australia and Director of Global Growth at ATP Innovations.

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

Piers Hogarth-Scott
Director
Digital Consulting
T: +61 2 9346 5551
E: piershs@kpmg.com.au

Luke Anderson
Director
Technology Advisory
T: +61 2 9335 8974
E: lukeanderson@kpmg.com.au

Peter Klement
Associate Director
Technology Advisory
T: +61 2 9335 8956
E: pklement1@kpmg.com.au

kpmg.com.au

Download on the App Store

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

April 2016. QLDN13934LOBS.