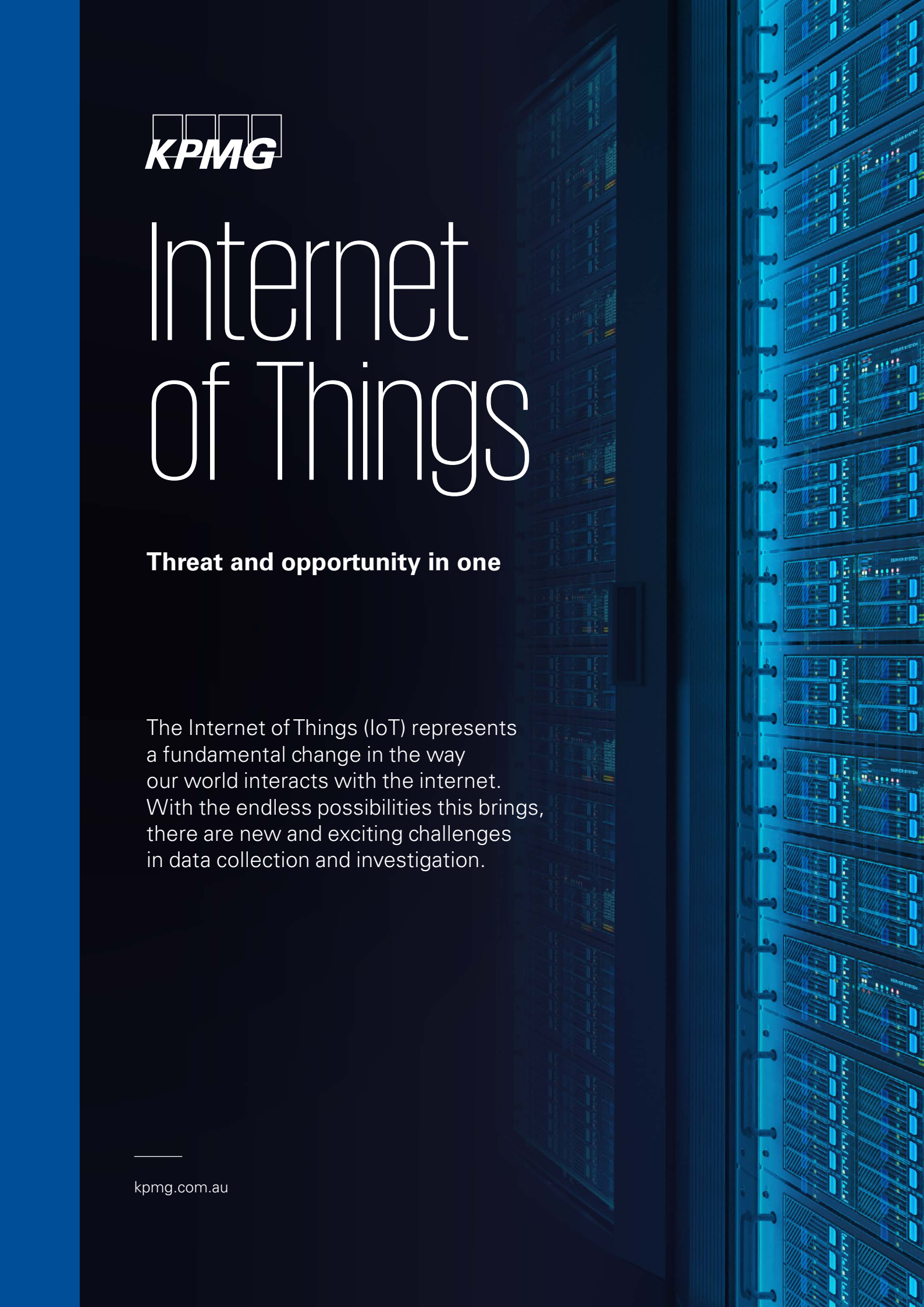

KPMG

Internet of Things

Threat and opportunity in one

The Internet of Things (IoT) represents a fundamental change in the way our world interacts with the internet. With the endless possibilities this brings, there are new and exciting challenges in data collection and investigation.

kpmg.com.au

Anatomy of an IoT attack:

1

At the 2015 RSA Conference, hackers demonstrated their plan to hack a power plant – a critical infrastructure target – utilising the IoT to obtain critical data from an employee's home environment.

2

Using social engineering and hacking software, they breached a smart oven connected to the home Wi-Fi network.

3

This access provided capacity to extend the breach to a mobile employee workstation, where passwords and confidential data regarding a power plant are stored.

4

This provided the hackers with administrative privileges and the potential for catastrophic damage to the power plant.

92%

of IoT users are concerned about security according to the 2015 KPMG IoT Survey.[7]

$445b

$445 billion is the estimated cost of cybercrimes globally each year.[8] The IoT will only increase this.

If your IoT technology is compromised, ensure that electronic evidence is handled appropriately. Due to the complex, interlinked nature of these networks, the information could be inadvertently accessed and contaminated.

Amend and optimise cyber policies and procedures in order to enable a resilient approach to the IoT and other relevant developments.

IoT investigations:

The IoT represents a significant shift in how we interact with data. The volume of information collected provides opportunities for seasoned forensic specialists to conduct investigations. The data will largely be located outside your own data centres, in the cloud, with third or fourth parties, or on (mobile) devices of employees or clients.

Develop a standardised platform within your business to ensure the maximum security of your IoT network. Look at what data is critical in terms of security and make sure this is adequately protected.

Containing an IoT breach is increasingly challenging. A forensic specialist should know that evidence is no longer restricted to a PC or mobile device, but can be found in vehicles, RFID cards, and even in a fridge.

A major challenge in the development of IoT technology is the enormous variety in systems used. Consider which systems are most critical to you and understand their structures so that adequate actions can be taken in the event of a breach.

IoT breaches:

In 2001, Vitek Boden was a disgruntled employee who presided over the Supervisory Control and Data Acquisition (SCADA) systems that managed a local Sunshine Coast council's sewage infrastructure. He hacked the nodes responsible for the flow of waste through pipelines causing several million litres of raw sewage to flood community parklands, hotel grounds and canals.

Boden's cyber-attack is considered Australia's first breach on critical infrastructure. In response, the Maroochy Shire Council has spent over $50,000 to upgrade security systems. With the rise of the IoT, many more systems will become similarly vulnerable.

A similar compromise occurred in 2010, but on a much larger scale. Dubbed the 'Stuxnet' worm, it was found in millions of computers globally, including traffic systems, power plants and hospitals.

Designed to target the Iranian nuclear centrifuges, it was able to modify the normal process beyond what was safe, yet could tell engineers that 'nothing was wrong'. The virus destroyed over 1,000 centrifuges and delayed Iran's nuclear program by 3 years.

173m
wearable devices owned by 2019 – a 100 million increase from 2015[1]

50b
devices connected to the internet by 2020[3]

90%
90 percent of new cars will have internet access in the next 5 years[5]

1.9b
1.9 billion smart-home devices sold by 2019, worth a total of $490 billion[2]

Over **2/3**
of consumers plan to adopt connected technologies by 2020[4]

6.2t
Projected value of IoT technology by 2025 up to $6.2 trillion[6]

The role of the KPMG Cyber and Digital Forensics team:

If your systems are compromised by a coordinated IoT cyber-attack, KPMG professionals will be able to examine data from new and unique sources, such as a smart oven.

The hackers will leave evidence of their actions within the IoT systems as they attempt to gain access and exploit more devices. Our experts will create a dynamic incident map and discover the vulnerabilities.

Due to the number of objects involved in an IoT breach, significant technical challenges exist. KPMG can help with navigating these scenarios, assisting in compliance and continuity of evidence.

We can assist with policies, processes and procedures, and test your IoT systems to plan for the future.

Gary Gill
Partner in Charge, Forensic
T: +61 2 9335 7312
E: ggill@kpmg.com.au

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

Stan Gallo
National Director, Forensic Technology
T: +61 8 9263 7347
E: sgallo@kpmg.com.au

1. http://www.onwindows.com/Article/smart-wearables-to-reach-1734-million-by-2019-48003
2. http://www.fool.com/investing/general/2015/02/06/17-internet-of-things-statistics-you-dont-know.aspx
3. http://www.cmo.com/articles/2015/4/13/mind-blowing-stats-internet-of-things-iot.html
4. http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#293f18342dc9
5. http://www.link-labs.com/internet-of-things-statistics/
6. http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
7. https://home.kpmg.com/xx/en/home/insights/2015/12/security-and-the-iot-ecosystem.html
8. http://www.mcafee.com/au/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

kpmg.com.au

Download on the App Store

April 2016. QLDN13947LOBS.