TMT ANALYTICS

Industry report

Technology

Telecoms Services

Industrials

Utilities

Consumer Cyclicals

Take-aways from CeBIT 2017

The growing pains of the Internet of Things

We recently attended one of the largest Enterprise Technology conferences globally, CeBIT in Hannover, Germany. The range of Technology verticals represented at CeBIT continues to be very impressive and includes sub sectors such as Data Analytics, Content Management, Artificial Intelligence, Cyber Security, Internet of Things, Virtual & Augmented Reality, (connected) Robotics and Industrial UAV's (drones).

In addition to the many presentations, round tables and seminars we attended, we also met with senior representatives of a.o. Microsoft, HP Enterprise, Nokia and Kaspersky to discuss legal, technical and operational issues in several of these sub sectors.

Augmented Reality will present major cost savings opportunities

While we believe Virtual Reality (VR) will be a killer app in the Computer Gaming industry, we believe Augmented Reality (AR) will have substantially more application areas in Industrial and Services settings, at least in the near to medium term. We expect AR will result in very substantial cost savings, for instance on complex production lines such as for car engines. Additionally, field maintenance of complex systems (e.g. lifts, power stations etc) can benefit tremendously from online availability of manuals and support through AR headsets.

It will take longer than expected for drones to become mainstream

With respect to drones, we definitely see many application areas for UAV's, such as geospatial imaging, scanning, short hop delivery etc. However, we also believe there are several major issues to be resolved before drones can become a widely-used tool in consumers' every-day lives. These issues including low altitude air space restrictions, privacy and security.

Key take-away: IoT security and data issues pose serious threats

Overall, we came across many interesting technological developments at CeBIT 2017. However, for us the key take-away is the threat posed by security and data issues surrounding the fast growth of the Internet of Things; a threat posed to companies and individuals alike.

In the current IoT land rush, basic device security has become an afterthought rather than a prime concern for many manufacturers and software providers, resulting in a large installed base of relatively unsecure IoT nodes in the field (e.g. home automation, smart meters, connected cars, toys, smart TV's etc). Unsecure IoT nodes have become a major staging area for massive cyber-attacks affecting both companies and individuals. Additionally, there is currently very limited clarity around ownership of data generated by IoT devices, while data privacy in the age of IoT presents completely new challenges for companies, especially in light of the upcoming **General Data Protection Regulation** (GDPR) in the EU.

Our main conclusion is that IoT-risks need to be an integral part of risk assessment, both for investors and any company active in the IoT space as well as any company deploying IoT functionality in their operations.

30 March 2017

Analyst: Marc Kennis
marc.kennis@tmt-analytics.com.au
+61 (0)4 3483 8134

Important things are forgotten in the IoT land rush

The Internet of Things (IoT) is the global network of devices, sensors, machines, appliances, vehicles, buildings etc connected such that they can collect and exchange information through a wired connection or wirelessly, e.g. through WiFi, Bluetooth, RFiD, NFC and 4G (Figure 1).

Figure 1: Interconnectivity of devices on the IoT

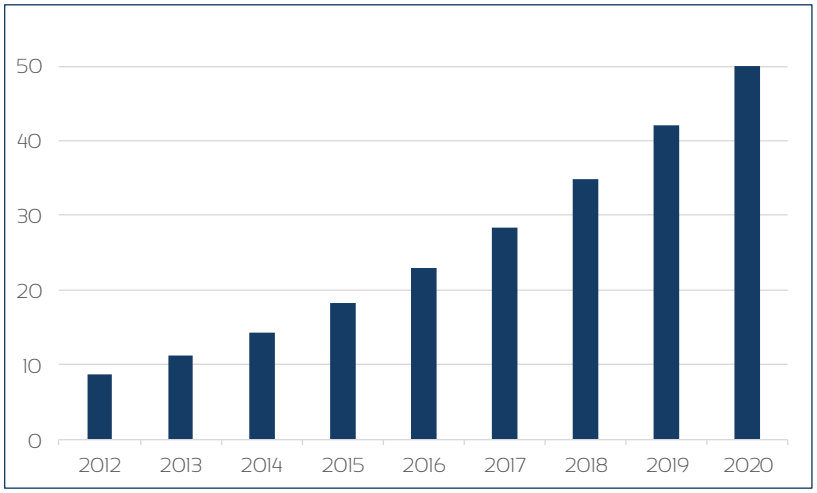
Source: Cerner, TMT Analytics

Common examples of IoT devices, also known as IoT nodes, include connected cars, wearables, remote wireless sensors, such as smart energy meters and agricultural sensors, smart phones, stand-alone digital assistants, such as Google Home and Alexa, laptops and desktop computers, home automation devices, industrial sensors in factories and many types of consumer electronics, such as connected toys, light bulbs and smart TV's.

The IoT is growing exponentially

Many types of devices on the IoT were previously not connected to the internet. Cars, watches and many home electronics devices, for example, have only started to be connected wirelessly to the Internet in the past couple of years.

Figure 2: The number of devices connected to the IoT (in BN)



Source: Kaspersky Labs, TMT Analytics

Because so many of these previously unconnected devices are now being provided with connectivity to the Internet, the growth of IoT has been very high. In fact, since the "inception" of the IoT in 2009 the number of connected devices has been growing exponentially and is expected to total more than 28BN devices by the end of 2017 (Figure 2). By 2020 the total number of connected devices is expected to amount to more than 50BN.

The IoT land rush leaves networks highly exposed

The commercial opportunity around the IoT is immense, as illustrated by the rapid emergence of entirely new product categories, such as wearable electronics, or wearables. Fitness and sports trackers, smart watches, and advanced combinations of hearing aids and Bluetooth in-ear headsets have become a multibillion dollar industry in the course of just several years. We have seen similar growth in Home automation and Industrial IoT applications, such as connected robotics.

Given this tremendous commercial opportunity it is no wonder that companies are very eager to launch new products in this space. However, in their rush to tap into these new market opportunities, we believe critical aspects of the IoT have tended to be overlooked by many companies.

> *Specifically, we believe security of IoT nodes, ownership of IoT-generated data and data privacy are the key weak spots of the IoT today.*

Security of IoT nodes leaves a lot to be desired

Many IoT nodes have small form factors, which limits the amount of functionality that can be packed into these devices. Typically, battery life, memory capacity, computing power and transmission bandwidth on wireless IoT nodes are very limited.

For most, if not all wireless IoT nodes, battery life is of crucial importance. While we can easily recharge a smart phone, many remote sensors, such as agricultural sensors and energy meters, will be out in the field for many years using the same battery. Therefore, low energy consumption is critical for commercial deployment, which limits the amount of processing that can be done on remote IoT nodes.

Furthermore, given the small form factor, both memory capacity and computing power are fairly limited on wireless IoT nodes. Limited memory capacity implies that these nodes need to transmit their collected data up to the Cloud on a very regular basis, while most data processing and analytics will be done off board, i.e. in the Cloud as well.

Combined with the aforementioned low battery capacity, it will be obvious that these two issues are a compounding problem for IoT device manufacturers.

Non-IoT specific Operating Systems and unsecure software add to the problem

We have only seen the emergence of IoT-specific Operating Systems in the last few years, such as Linux-based Operating Systems, ARM mbed, FreeRTOS and the recently released KasperskyOS for IoT.

Prior to that, IoT devices would typically run on generic Operating Systems, many of which are known to have vulnerabilities. Consequently, there is a substantial installed base of IoT devices out there running on relatively unsecure Operating Systems.

Software often lacks basic security features

In addition to the use of non IoT-specific Operating Systems, often the software used in IoT devices lacks basic security features, such as proper encryption or password protection. In fact, sometimes IoT devices' passwords are coded into the devices' software.

Many attacks launched from IoT devices

Given the inherent vulnerabilities of legacy IoT devices, i.e. with older Operating Systems, it will come as no surprise that IoT nodes, such as printers and home automation devices, have been used a lot to launch cyber-attacks.

Recent distributed denial-of-service (DDoS) attacks have been carried out using slaved IoT nodes, while hacking sessions at Def Con exposed around 50 vulnerabilities in connected door locks and solar panels.

And as the infamous hacking of a connected Jeep Grand Cherokee in 2015 illustrated, unsecure IoT nodes can also serve as a way into larger hosts. This specific hack resulted in the recall of 1.4M cars.

> *Even today, despite improved security measures, there are still more than ten ways to attack a connected car.*

Despite security improvements, the IoT will remain a source of cyber-attacks

In the past, many IoT devices have been rushed to the market with security aspects taking the back seat, in our view, in particular in the consumer segment. And even though this seems to be changing, we believe these legacy IoT security issues will continue to facilitate large scale cyber-attacks going forward.

The IoT is a network after all and attackers will continue to seek out the weakest links to stage their assaults, as the case of hacked teddy bears illustrates (Figure 3). In February 2017, it became apparent that voice recordings of conversations among children and their parents, made by a range of internet-connected teddy bears and stuffed toys, had been accessed by hackers. They also gained access to passwords and email addresses.

Additionally, it turned out that the recordings had been made without the parents' consent to begin with, which touches on the data privacy issues we will discuss below.

FIGURE 3: CLOUDPETS CONNECTED TEDDY BEARS

Source: CloudPets, TMT Analytics

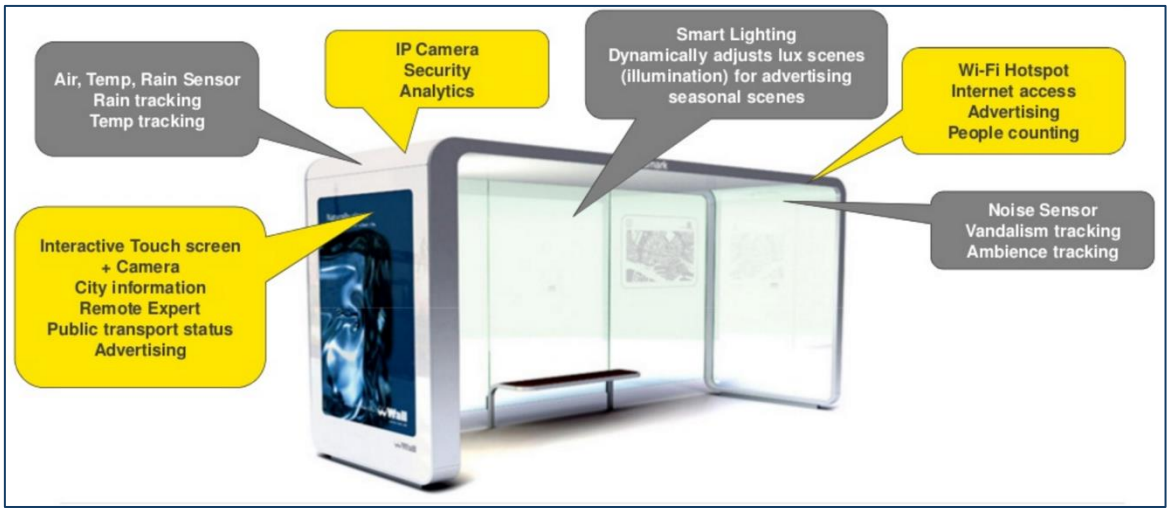
Data ownership in the age of IoT is murky

The business models of companies such as Google and Facebook are well-understood; in exchange for use of their platforms, users hand over a lot of their personal information by accepting the respective privacy policy. This personal information may be used for commercial purposes. In the IoT space, however, data ownership is less clear.

Who owns IoT node-generated data?

The best way to underline the importance of this question is to use an example: Imagine a smart bus shelter, i.e. a bus stop with a roof, an LCD display for real-time information, such as time tables, expected bus arrival times etc, as well as for advertising, news and tourist information. Additionally, these shelters can have a multitude of sensors and cameras for various purposes.

FIGURE 4: CONNECTED BUS SHELTER



Source: Cisco, TMT Analytics

The bus stop will have a data connection, most likely 3G or LTE, to facilitate content being displayed on the display. Additionally, it will have Wi-Fi small cell for passengers to connect to.

The value of the data generated by the IoT nodes integrated into this bus shelter will depend on what it will be used for. For instance, data derived from passengers' Wi-Fi connections, their smart phones' unique device identifier and geo-tags will be highly valuable to the outdoor advertising company that owns (or has provided) the outdoor display.

It will use passenger information, such as demographics and lingering data, and overlay it with other sources, e.g. from Google and Facebook, to drive advertising revenues through highly targeted ads during different times of the day.

Ownership of all this data is less clear

One could argue that because the outdoor advertising company has provided the display in return for passengers' data, which is a common business model for outdoor advertising, the ad company owns the passenger data generated by this bus shelter. However, the bus company, the network operator, the hardware and software providers and the IT service provider may also lay claim to the data generated from the various integrated IoT nodes, not to mention the passengers whose data is being harvested.

Regulation needed

While data ownership will, to some extent, depend on the business model used, there are many unclarities surrounding this topic, which need to be sorted to facilitate rapid adoption of advanced IoT applications, such as Smart City furniture like connected bus shelters.

These data ownership issues also apply to much simpler IoT applications, such as smart energy meters, wearables and Home Automation.

> *Without exception, all industry participants we spoke with during CeBIT 2017 indicated that regulation will be required, preferably on a global/industry-wide scale, in order to streamline data ownership issues.*

However, we believe the industry is still a long way off from overarching regulation around IoT node-generated data ownership.

Data privacy presents new challenges in the age of IoT

In line with data ownership issues, data privacy is an equally important issue in the IoT age. Even though a lot more regulation is in place to manage data privacy compared to regulation for data ownership, we believe the IoT presents privacy challenges not dealt with before.

For instance, the fact that many manufacturers of consumer-related IoT devices do not have proper privacy policies in place, doesn't mean they can freely use the data generated by these devices.

Furthermore, because in many situations it is unclear who actually owns certain data generated by IoT nodes, maintaining privacy of this data may become the proverbial hot potato, with industry participants pointing to one-another in privacy breach situations.

New EU regulation, in effect from May 2018, can also impact non-EU companies

New and far-reaching regulation in the EU is a good example of the challenges that companies, active in the IoT space, will be confronted with from mid-2018.

The EU's **General Data Protection Regulation** (GDPR), which will replace the EU's twenty-two-year-old Data Protection Directive, affects data retention and privacy from six different angles:

1. The right to be forgotten; similar to how Google is required to delete specific, personal information from its caches if the relevant person requests this, the right to be forgotten applies to an individual's specific data as well. In other words, IoT players retaining data will need policies in place to remove user specific data.
2. Privacy by design; data holders will be required to implement appropriate technical and organizational measures to protect personal data against unlawful processing, which is a new requirement. From the outset of any product or process development, companies will need to design compliant policies, procedures and systems using "state of the art" technology, i.e. the most up-to-date technology needs to be used for this purpose.
3. Risk and impact assessment; this element of the GDPR requires data controllers to conduct a data protection impact assessment for high-risk processing activities, which may result in the requirement for stronger encryption, pseudonymizing or anonymization of data. Data holders and processors need to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

4. Data breaches; under the GDPR a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. This is a much broader definition than the US definition. A breach must be reported to the supervisory authority within 72 hours after the data holder has become aware of it, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons. The latter will undoubtedly become food for lawyers.
5. Consent to process a user's data; the GDPR requires consent to be expressed by a statement or by a clear affirmative action for each data processing operation. Consequently, silence, pre-ticked boxes or inactivity on the part of data owners will not be sufficient for data processors. Furthermore, withdrawing consent must be made as easy as it is to give consent. i.e. a consent withdrawal application should be readily available for data owners.
6. Data portability; data owners will have the right to data portability, which aims to increase owners' choice of online services. This may mean that the data controller could be required to transmit the data directly to a competitor.

> *In our view, these six elements of the new EU legislation will have a profound impact on the IoT world, given the current lack of security of IoT nodes and the absence of any sort of privacy policy around many IoT devices being sold today.*

Because the GDPR is EU regulation, it affects any company active in the EU, e.g. with local offices and facilities, selling into the EU and processing EU data owners' information. In other words, the GDPR is quite far-reaching.

Furthermore, fines for non-compliance can be very high, i.e. up to 4% of a company's global revenues with a maximum of EUR 20M.

> *Given the current state of IoT device and data security, unclarity around data ownership and weak or missing privacy policies, we believe the GDRP may turn out to be a brick wall that many IoT-related companies will run into come 2018.*

Three near term challenges for IoT players

Through our discussions at CeBIT we have identified three key challenges the IoT sector will need to overcome in the near term.

Who owns the IoT node-generated data?

Firstly, a lot more clarification will be required around ownership of data generated by IOT nodes. Industry-wide regulation and standardization will be required. And while this is being worked on, we expect this will remain work-in-progress for some time to come.

Security, security, security

Secondly, security of IoT nodes needs to be substantially improved upon, both at the device level and at the network level. Specifically, further standardization of security protocols will be required.

This pertains mostly to the way IoT devices are onboarded within a network, e.g. a home WiFi network. A secure middleware layer needs to be able to identify and authenticate devices in order to onboard applications and individual IoT devices without these devices being able to directly communicate with any of the applications, unless an application has specifically subscribed to a certain IoT device.

Furthermore, the wireless edge of the IoT needs the ability to get security patches and software updates over the air, which is currently not possible for many wireless IoT nodes.

Additionally, more processing power and memory capacity will be required at the node to facilitate more data analytics at the edge of the IoT. This is important for two reasons, firstly to enable IoT nodes to perform more security checks at the node rather than in the core of the network. This should prevent more cyber-attacks from IoT devices. Secondly, segmenting essential from non-essential data at the node will limit the amount of data transmission from the node, allowing for less transmission bandwidth at the node and less storage capacity at the network core (data centers).

Scalability of the network

Today's structure of the IoT consists of many different verticals, each with largely different protocols, applications and infrastructures. This fragmented structure limits the scalability of the network. Therefore, more standardization is required in this respect. Ideally, a horizontal infrastructure with shared functionality is created, i.e. standardized security and onboarding protocols on top of which vertical applications can be deployed. Such a single platform will be much more scalable than the current stand-alone applications.

Conclusion: IoT-risks to be an integral part of risk assessment

Our key take-away from CeBIT 2017 is that we are only at the early development stages of the Internet of Things. As we continue to move towards a programmable world, substantial hurdles will need to be taken, especially around security of IoT devices.

Current security issues impact all IoT-related players, be they manufacturers, software providers, operators, device owners, data centers, telco companies as well as the average consumer.

Include specific IoT risk assessment in investment decisions

From an investment point of view, we recommend to look at listed companies from a specific IoT-angle, i.e. how are companies mitigating the risks they run in the areas of device security, data ownership and data privacy.

In our view, these issues are relevant all the way up a company's supply chain, e.g. where supply of device components is concerned. And with penalties in the EU of up to 4% for non-compliance with the new data privacy and security legislation, the monetary impact can be very substantial, not to mention the reputational impact of data breaches and hacks.

Check your supply chains, protocols and policies

Data ownership issues will affect every company in the IoT space, while the new EU legislation around data privacy will affect every company operating in the EU, even if the company itself is not EU-based. Furthermore, security of IoT nodes should be every company's concern, either as a consumer of these devices or as a supplier in some shape or form.

Consequently, we believe companies would be wise to check and double-check their supply chains, protocols and policies to minimize business risks around new and existing IoT infrastructure.

GENERAL ADVICE WARNING, DISCLAIMER & DISCLOSURES

The information contained herein ("Content") has been prepared and issued by TMT Analytics Pty Ltd ABN 17 611 989 774 ("TMT Analytics"), an Authorised Representative (no: 1242594) of Bellmont Securities ABN 47 119 852 890 AFSL 331625. All intellectual property relating to the Content vests with TMT Analytics unless otherwise noted.

DISCLAIMER

The Content is provided on an as is basis, without warranty (express or implied). Whilst the Content has been prepared with all reasonable care from sources we believe to be reliable, no responsibility or liability shall be accepted by TMT Analytics for any errors or omissions or misstatements howsoever caused. Any opinions, forecasts or recommendations reflect our judgment and assumptions at the date of publication and may change without notice. TMT Analytics will not accept any responsibility for updating any advice, views, opinions or recommendations contained in this document.

No guarantees or warranties regarding accuracy, completeness or fitness for purpose are provided by TMT Analytics, and under no circumstances will any of TMT Analytics, its officers, representatives, associates or agents be liable for any loss or damage, whether direct, incidental or consequential, caused by reliance on or use of the Content.

GENERAL ADVICE WARNING

The Content has been prepared for general information purposes only and is not (and cannot be construed or relied upon as) personal advice nor as an offer to buy/sell/subscribe to any of the financial products mentioned herein. No investment objectives, financial circumstances or needs of any individual have been taken into consideration in the preparation of the Content.

Financial products are complex, entail risk of loss, may rise and fall, and are impacted by a range of market and economic factors, and you should always obtain professional advice to ensure trading or investing in such products is suitable for your circumstances, and ensure you obtain, read and understand any applicable offer document.

DISCLOSURES

TMT Analytics has been commissioned to prepare the Content. From time to time, TMT Analytics' representatives or associates may hold interests, transact or hold directorships in, or perform paid services for, companies mentioned herein. TMT Analytics and its associates, officers, directors and employees, may, from time to time hold securities in the companies referred to herein and may trade in those securities as principal, and in a manner which may be contrary to recommendations mentioned in this document.

TMT Analytics may receive fees from a company referred to in this document, for research services and other financial services or advice we may provide to that company. The analyst has received assistance from the company in preparing this document. The company has provided the analyst with communication with senior management and information on the company and industry. As part of due diligence, the analyst has independently and critically reviewed the assistance and information provided by the company to form the opinions expressed in the report. Diligent care has been taken by the analyst to maintain an honest and fair objectivity in writing this report and making the recommendation. Where TMT Analytics has been commissioned to prepare Content and receives fees for its preparation, please note that NO part of the fee, compensation or employee remuneration paid will either directly or indirectly impact the Content provided.

RECOMMENDATIONS

TMT Analytics' issues a BUY recommendation in case of an expected total shareholder return (TSR, share price appreciation plus dividend yield) in excess of 25% within the next twelve months, an ACCUMULATE recommendation in case of an expected TSR between 5% and 25%, a HOLD recommendation in case of an expected TSR between -5% and +5% within the next twelve months and a SELL recommendation in case of an expected total return lower than -5% within the next twelve months.