Anna Tarabasz
Uniwersytet Łódzki

The Internet of Things – Digital Revolution in Offline Market. Opportunity or Threat?

Summary

According to eMarketer forecasts for the year 2015, there are 3.07 billion of Internet users worldwide, what constitutes the 42.4% penetration ratio of this medium, whereas there are 15 billion of already plugged devices. Moreover, this number will increase rapidly, as 200 billion of such items are expected by the end of the year 2020. The potential economic impact by the growth annual ratio of the Internet of Things (IoT) is estimated to achieve between $2.7 to $6.2 trillion by 2025. The largest influence is anticipated for healthcare and manufacturing sectors.

The main aim of this article is to present the innovative approach of the IoT idea, ennumerate juxtaposition of its opportunities and threats as well as to indicate its inner potential still being dormant. In this regard the paper will present exemplifications of smart objects and the idea of sensors and locators, that underlie creation of intelligent shopping, communication integration, effective buying process, automatic alerts, personalised, intelligent packaging or profiled advertisement in VOD. Therefore the Internet of Things exerts an indisputable positive influence on changing the paradigm of the market, product, offer, communication, and business management. As unfortunately "every rose has its thorn", similar regularity applies to the IoT, in relation to cyber attacks wich involve application of force to capture, disrupt, deny, degrade, destroy, or manipulate computing and information resources due to low security level. The remote access to smart devices may though lead to potential malicious attacks on employees, health information leaks, and attacks on key executives in order to influence or control the financial stability of the organisation. Therefore, the article will be an attempt to compare the potential opportunities and threats arising from the IoT idea.

Key words: Internet of Things, IoT, smart objects, wereables, technological innovation consequences, brick & mortar market, click & mortar market.

JEL codes: L86, O33

Introduction

The Internet of Things (IoT), interchangeably known as the Internet of Everything (IoE) or the Internet of Objects (IoO) as a phenomenon significantly exceeds beyond the original expectations. What was initially concidered to be a "technology trigger" in the Gartner Hype Cycle for Emerging Technologies in 2011 (Postcapes 2011), three years after, in 2014, constitutes the major point in "peak of inflated expectations" (Postcapes 2015) and its mainstream adoption is anticipated for incoming 5-10 years

Despite the fact of increasing investments in this field, and estimated potential of the IoT to be between $2.7 to $6.2 trillion per year by 2025, yet still 99% of existing devices are not connected to the Internet. The importance of this solution implementation and forthcoming benefits are well reflected by the fact, thatthe process of systematic connecting existing devices to the Internet is nowadays called "the electrification of the 21st. Century".

Even though with our knowledge and development level we are only at the tip on an iceberg, trying to predict the unknown, as the technology is developping according to chain reaction scheme. As rightly pointed Hess (2014) you can do as little or as much with IoT as you want. How much more is only left to your imagination and to your budget.

But considering the IoT only in terms of a costless blessing is an oversimplification of existing reality. The other side of the coin reveals the problem of low information security, that may encourage hackers to steal sensitive data. This in turn may lead to crises of different range - from minor ones, like publicating private health information to major including, like influencing political decisions or impacting the financial condition of enterprise.

The main of this article is to present the innovative approach of the IoT idea, ennumerate juxtaposition of its opportunities and threats as well as indicate its inner potential still lying dormant.

The idea of Internet of things

The autorship of the term is assigned to Kevin Ashton, who used it in 1999 (Ashton 2009) while working in P&G company in presentation for the executives. But the practical application of previously described theoretical solutiontook place ten years after, at the turn of the year 2008/2009 (Cisco IBSG & Evans 2011).

There are multiple definitions of this idea. For example quite versatile approach is presented bythe International Telecommunication Union's Global Standards Initiative (ITU 2012), that is defining the Internet of Things is, as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. They also include in their approach a broader perspective, in which the IoE can be perceived as a vision with technological and societal implications. But for the average John Doe, the Internet of Things (IoT) is constituting new attitude, favoring redefinition of market, buyers, users and the range of products. In this regard such approachremains rather closer to Geer's (2014) point of view, who simply defines it as a mass of billions of connected [to the Internet] devices: from cars to wireless wearable products.

Yet it has to be underlined, what was clearly done by Best Computer Science Degrees (2015), that not all of IoT things are directly connected to the Internet. Some objects, such as sensors, communicate wirelessly to each other in M2M (machine-to-machine) system over a localized network, and to some sort of base device, which is Internet-connected. Other

communication forms include equally machine-to-person (M2P), P2M (person-to-machine) as well as communication between person-to-person.

The complicated technical background establishes, from the point of view of an average user, the ubiquitous network of smart objects, allowing human-to-human (H2H) communication, at the same time in reality reduced to M2M or O2O (Object-to-Object) information interchange. Such data flow, acording to McKinsey (2013), constitute three steps in Internet of Things applications: (1) capturing data from the object (for example, simple location data or more complex information), (2) aggregating that information across a data network, and (3) acting on that information - taking immediate action or collecting data over time to design process improvements.

Worth noting seems also to be the Chaouchi's (2010) approach,who apart from confirming the above mentioned approach, rightly stresses, that the IoT is rather about designing new services and generating new streams in the communication value chain. That is why he conciders it to be one step further on the leading path to a smart world with ubiquitous computing and networking. From such point of view, IoE constitutes a meeting point between the real and virtual worlds, especially when combined with other technologies, such as sensor technology or mobile communication. He also emphasizes the importance and complexity of the phenomenon: implementation of RFID (radio-frequency identification) technology, sensors, nanotechnology and robotics. All this in order to make the IoT services an interdisciplinary field where most of the human senses are somehow reproduced and replaced in the virtual world.

Enormous are the possibilities given in this regard by wireless communication technologies for non-autonomous things, like for example sensors. These include amongst others RFID (Radio Frequency Identification), NFC (Near Field Communication), Wi-Fi, BLE (Bluetooth Low Energy), XBee (radio module), Zigbee (low-power digital radio) or Wireless M-Bus (protocol software allowing RF communication) amongst others. To communicate via the Internet these devices may require an IP (Internet Protocol) address to uniquely identify particular object. These almost "foreign sounding" names are used while product identification&tracking, asset management, access control, payments, monitoring, location-based services and many more. The implementationof their possibilities takes place not only in B2Binteractions, but is introduced into e-Commerce, entertainment, finance, health, IT, real estate, sports, travel and many more. But the more difficult to understand it becomes for an average bread eater, the more covered by the "graynes of everyday life" is the unnoticed miracle of conscious, technical process, occuring in the ease of use, 24/7 indissoluble presence of smart objects and due to the communication convinience.

Digital revolution influencing offline market

Smart objects, sensors, locators, wrist-bands or arm-bands and compatible with them appliacations, underlie the creation of intelligent shopping, processes integration, effective buying process, automatic alerts, personalized, intelligent packaging and profiled advertise-

ment in VOD. Such activities occur already at superior scale in smart cities, transportation and environmental domains. At the same time they only reveal the proverbial "tip of an iceberg", as the remaining part, that constitute the majority of the phenomenon, remains hidden (Tarabasz 2015).

The innter potential of the IoT, still lying dormant, is visible while creating a simple juxtaposition. Currently there are over 3 billions of Internet users worldwide and at the same time there are 25 billions of connected objects (Cisco IBSG 2011) that in overall constitute the Internet of Everyting. But the true potential yet is to be about available. Far more important is here the enormous growth possibility. The impressive data concerning the number of connected items, constitute solely the 1% fraction of all existing devices, that could be networked.According to eMarketer (2015) forecasts for the year 2015, the 3.07 billions of Internet users worldwide constitute 42.4% penetration ratio of this medium, whereas the previsioned number of plugged devices will increase rapidly, as according to Best Computer Science and Postcapes [2015] 200 billions of such items are foreseen by the end of the year 2020.

These numbers quoted above are not only to show the magnitude of target users group, but more importantly to indicate the power of a real market value they constitute. McKinsey [2013] in its reports estimates the IoT potential economic impact growth annual ratio to be between $2.7 to $6.2 trillion per year by 2025. According to previously quoted Best Computer Sciences Degrees (2015) $4.8 trillion was the global IoT market (technology and services, gross revenue) for the year 2012. Moreover, this type of solution will increase rapidly, as the total of $8.9 trillion is the expected market worth for the year 2020, which gives a CAGR (Compound Annual Growth Rate) of 7.9%. According to already mentioned McKinsey's report (2013) the largest influence into the IoT market worth is anticipated in health care and manufacturing sector. Worth emphasizing is the fact, that the first of enumerated sectors will provide an economic impact of $1.1 trillion to $2.5 trillion per year by 2020.

These massive statistics, previsions and listed data shall not be treated as the proverbial foretelling from the crystall ball, but rather preparing for the ineviteable. The digital revolution of smart objects, wereables and the IoE is, in a clearly visible manner, influencing the current offline market. According to the report of Sales Mango & Benhauer Marketing Technologies (2015) the sectors in which the IoT developes nowadays the most dynamicly are fitness, FMCG (with particulcar emphasis for bio and eco products), home appliances, lifestyle devices, smart parenting, TV, ecology and communication and the trend predicted not only is entirely positively verified, but very often occur with a large surplus.

The practical application of the IOT phenomenon

The IoE creates a meeting point between a difficult to understand theory and easy to handle practice. The ubiquitous computing and devices miniaturization favors the proliferation of smart objects.More and more often people are willing to monitor everything and everywhere for further improvement. For example Kolibree is the world's first connected

toothbrush, which collects data about habits and though reports a need to improve; especially bought by parents to their children. HAPI fork is a networked fork, which helps alerting at too rapid eating, supports introducing new nutritional habits and monitor them. Sportsmen already use Biometric Smartwer by OMsignal, that allows not only to minitor the heart rate and breath, but equally acts as calories and steps counter with fitness tracker function. All this to train in a more effective and intelligent way…

There are paramedical solutions like Adhere Tech: an intelligent packaging for drugs, responsible for verification on receiving doses of medicament prescripted by the doctor to its patient. From this sector worth mentioning is the project of Google's soft smart lenses, still in testing phase, that measures the glucose level. Such solutions are more and more often present in smart parenting and eldery people care – smart clothes or diapers, which inform about inapropriate temperature and humidity. But it is far behind only simple measuring solution and alerting when reaching certain level. While Pixie's Smart Diaper with QR codes and colorful squares allow to measure hydration level, possible diabetis, kidney problems, bacteria infection etc. of kids, Sensidry is dedicated for adults with the incontinence problem. Here monitoring is rather about restoring dignity for the beloved ones, that cannot anymore simply communicate their physical needs, but still are aware and concious and dedicated to hospital staff that is notified online about the change obligation.

Nowadays smart objects go one step further and are becoming independent: either they launch themselves, like Kapture and Autograph (for the perpetuation of special moments as picture, audio or video form) or disable, like Nest, an intelligent thermostat, that learns user's preferences and behaviors in addition switches itself off, when nobody is at home. But what becomes the most important, the IoT extends far beyond simple items and creates a real network of omnipresent smart objects, that instead of exchanging information, may in close future independently draw conclusions. Already available refrigerators (products of Electrolux, LG, Samsung or Whirlpool), can be remotely turned off or put into vacation mode, thenalso warn, when product ends or is approaching its "best before" date. Currently the designers are about to introduce devices integrated not only with function of creating the shopping list according to our dietary habits, but also online shopping capability from chosen company while the refill need is approaching!

The number of connected objects is increasing. Very often this online intelligence is granted to items, that are not trully desired by the customers. The presented below juxtaposition (cf. Table 1) lists types and examples of smart objects, divided into three groups according to the level of their suitability do buyers' needs. Worth stressing is here the fact, that categorization results come from Affinova (2015) research, conducted among 800 US adults, aged 18-54 and presents each time a general approach, not only the opinion of customers group using the particular product.

Devices from fitness group, are now, beyond smartphones and tablets, top-selling smart-objects. Depending on their complexity, may monitor the physical activity (Apple Watch, Sony SmartBand, Basis Peak, LG Watch Urbane), track progress in performed exercises or movements intricacy (Notch, Garmin Forerunner), and even arrange training plans (Tao

Table 1

Examples of the most&least wanted smart products according to consumers

mosty wanted		somewhat wanted		least wanted	
	**refrigerator** – enables remote viewing of its contents, recommends recipes based on stored items (*Electrolux, LG, Samsung, Whirlpool*)		**coffee maker** – synchronized with an alarm clock or simply remotely controlled (*Mr. Cofee, Grind*)		**razor** – sends an alert when the blade needs to be replaced or collects data for shaving pattern improve (*Eclipz Smart Razor*)
	**light bulb** – turns off when no one is nearby, can be remotely activated (*LIFX, Ilumi*)		**oven** – detects when food is done and sends a mobile alert (*Smart Oven Breville, Intelligent Oven June, Samsung*)		**baby diaper** – sends an alert when the diaper needs to be changed (Pixie *Smart Diaper, Sensidry – for adults' problems of incontinence*)
	**sprinkler system** – monitors weather over time, determines when to turn on and shut off (*Skydrop, Rachio, Lono, Cyber Rain*)		**vacuum** – cleans without human involvement and can be remotely activated (*Neato BotVac*)		**toothbrush** – tracks brushing habits and sends data to the user's dentist (*Kolibree*)
	**scale** – aggregates data from other devices and provides a constantly updated personal health plan (*Fitbit Aria, Withings Body Analyzer, iHealth, Bellabeat, Xiaomi Mi Smart Scale*)		**packaged food** – sends an alert when the item is on sale and displays nutrition information for a specific amount of food determined by the user (*till now simple TTIs like MonitorMark, TimeStrip, Fresh-Check, CheckPoint, not oferring sales option or nutrition information*)		**wine bottle & stopper**– sends an alert when the wine's flavor is best and, once opened, indicates when it is no longer suitable to drink (*Digital Cork, Smart Wine Bottle, by Thinfilm&G World system, authenticating the bottle origin and fact of beaing originally sealed*)
	**tap water filter** – automatically shuts off when nothing is in the sink and tracks water usage from all connected faucets and shower heads (*Smart Faucet, Ozner*)				
	**laundry washer and dryer** – sends an alert when the cycle is done, can be remotely activated (*LG, Samsung*)				

Source: own elaboration, based on: Affinova (2015).

Wellshell). Not only they can passively monitor and present interesting data (like Tinke, that i.e. indicates heart rate, blood oxygen level and breathing rate, by simple thumb touch), as the range of their possibilities grow continously. The most interesting is the fact, that slowly they become fully independent devices, that do not need to have, as so far, a continuous smartphone connection.

The above-mentioned solutions only serve to exemplify the possibilities of phenomena on a micro scale. In fact only single objects were shown, of which full potential is visible only while combined into groups. If, however, talking about sets of beacons, sensors, and detectors, even the space around will come alive and become intelligent. As an example, case studies of Smart Cities based on London and Helsinki shall be presented. In London Underground so-called big data incoming from sensors monitoring parameters like: temperature, vibration, humidity etc. are available in one central location in order to provide access to needed information on mobile applications, via a Web browser, or through text alerts (Microsoft 2014). These information in the aging transport system are about to improve customer service, prevision about faults and inconviniences. According to Cruz (2014) basing on these indicators, the operational efficiency was increasedby 30% over three years.

In case of Helsinki Bus Transportation effectiveness was improved based on ability to capture and track the traffic data, drivers' performance and gas usage. The company obtained 5% savings in fuel costs due to more careful driving and improved maintenance. But more impressive this number becomes, when realizing, that the company uses approximately 3 million gallons of gasoline per year, in a country where gas can cost up to three times as much as it does in the United States (Bhandari 2014).

Not all gold that giltters?

Ability to track everything almost everywhere, operate objects remotely and instantly monitor obtained results seems seductive. Unfortunately as the proverbial "every rose has its thorn", similar regularity applies to the IoT in relation to potential cyber attacks. According to Covington & Carskadden (2013) these mayinvolve application of force in order to capture, disrupt, deny, degrade, destroy, or manipulate computing and information resources, due to low security level. The remote access to smart devices may though lead to potential malicious attacks on employees, health information leaks, and attacks on key executives for influencing or controlling the financial stability of the organization.

Vulnerability to hacking attacks occurs mainly due to insufficient security of smart objects. The major problem remains mainly software, which is not so often updated as operation systems in PCs and dedicated for them further patches, aimed at closing, or hiding weaknesses as well of the device itself as of its processes. Unfortunately the market competition heads only in one direction. At first is about implementation of a unique solution (which not comes along with universal software), then appears the question of imitating, copying, and costs reducting. Both of these approaches could become a flashpoint for the device and potential gate to data theft or manipulation.

CSO, as an orgnisation providing news and multiple analysis on broad range of security and risk management topics,stresses the problem of PII (Personally Identiafable Information) leakage, spoofing (posing as smart device), snooping&manipulating data (unauthorized access & false changes) or simple spying competitors with the registered video from the wereables. Even though, the IoE beneficiary all time using smart objects shall be concious and aware of potential "Big Brother" that is still watching, everyday examples of threats in this regard are not that sophisticated. For the year 2015 CSO indicated 5 major threats for the IoT devices (Geer 2014), that are juxtapositioned below (cf. table 2).

Table 2

Top 5 major threats for the IoT devices

No.	Smart appliance	Threat type	Description
1.	in-car WiFi	spoofing PII leaking SPI leaking	in-car wiFi turns car into mobile hotspot, connecting passengers smartphones, tablets etc. to the Internet. lack of firewall allows spoofing, when hacker poses itself as the car and grabs information like credit card data, contacts, photos, documents, notes, aplications logins etc.
2.	mHealth apps/ mobile medical devices	PII leaking	poor patching mechanism for mobile Windows allow for viruses and data tracking, further occuring as health information leaks, malicious attacks on employees, especially on key executives in order for financial destabilization or influencing/controlling a company
3.	wereables/ Google Glasses	snooping spying	such smart objects automatically connect to the Internet, often with poor security solutions. wereables containig built-in camera may imperceptibly transfer (in the video and audio form) confidential corporate information and intellectual property
4.	retail inventory monitoring&control M2M	snooping DoS attacks SQL injection data manipulation	inventory management technologies include inexpensive 3G cellular data transmission on packages. while connecting to the Internet, transmitters make these applications vulnerable to Internet-based attacks, which may include data manipulation, like SQL code injections by changing the level of stocks and though simply lead to products shortcomings within the market. motivated by blackmail, revenge or simple activism, hackers may create a DoS (Denial of Service) attack, which is an attempt to make a machine or network resource unavailable to its intended users
5	drones for non-military use	buffer overrun SQL injections spying	unmanned aircraft rely on vulnerable telemetry signals, allowing for taking over the control of drone or at least being in possession of video transmission, taking high resolution photos, looking through windows i.e. for sensitive data (passwords etc.), or plant high fidelity microphones for eavesdropping outside of sensitive rooms (conference rooms, CEO offices)

Source: own elaboration, based on: Geer (2014).

The above mentioned threath types reveal a very small area availiable within a wide range of possible hacking attacks to smart objects. Aside from the fact of multiple existing bugs and software imperfections, often missing updates and patches, the biggest problem in utilizing the benefits of IoT is, as always, the human factor. The majority of Internet users are aware of the existence of the phishing phenomenon, draw attention to the presence of security certificates (Verisign) and HTTPS code with SSL / TLS encryption, even if such action is limited only to presence verification of "the green padlock" in the browser window. Unfortunately, however, in the case of smart objects and the IoT our awareness both on the level of security(which are often of poor quality, or simply are missing) and lurking hazards is low or even nil.This may entail the risk not only of losing sensitive data, but more often is synonymous with real financial losses.

Conclusions

The incontestable advantages of the Internet of Everything and constituting it connected smart devices alreadyinfluenceincreasingly and more willingly use the technology of tomorrow in everyday life. With the Internet of Objectsand big data available at fingertips, more and more items can be operated remotely and though the concept of "intelligent and connected home" is no longer just an illusion of sci-fi. People can work faster, more efficiently and effectively. Also theybecome better workers, parents and athletes. As Covington & Carskadden (2013) rightly point, the Internet of Things will bring many great new advances, including whole new ways of thinking about and interacting with our world. However, with these opportunities come equally many challenges in the field of information security, what in overall will require continous research and development of new approaches for ensuring required safety, security, and privacy. For this particular reason, every company following the new technological wave of the IoT, constituting the eletrification ot the 21st. Century, shall perceive not only of possible advantages as fast growing and valuable market, but be equally aware of its potential drawbacks and though is obliged to follow policy of sustainable development in this regard.

Bibliography

Accenture Interactive, & Acquity Group (2015), *The Internet of Things: The Future of Consumer Adoption,* https://www.accenture.com/us-en/insight-internet-things-future-consumer-adoption [access: 20.10.2015].

Affinova (2015), *Innovation Trend Watch. The Internet of Things. Can it find a foothold with mainstream audiences today*? http://iofthings.org/s/Internet_of_Things_Report__Web_.pdf [access: 21.11.2015].

Applegate S.D. (2012), *The Principle of Maneuver in Cyber Operations*, (in:) Czosseck C., Ottls R., Ziolkowski K. (Eds.), *4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallin.

Ashton K. (2009), *That 'Internet of Things' Thing*, "RFID Journal", http://www.rfidjournal.com/articles/view?4986 [access: 12.08.2015].

Best Computer Science Degrees (2015), *Understanding the Internet of Things: Towards a Smart Planet*, http://www.bestcomputersciencedegrees.com/internet-of-things/ [access: 10.06.2015].

Bhandari P. (2014), *How the Internet of Things is helping "smart cities" improve public transportation*, http://blogs.technet.com/b/openness/archive/2014/06/05/internet-of-things-smart-cities-improve-public-transportation-.aspx#.Vdcewfntmko [access: 21.08.2015].

Chaouchi H. (2010), *The Internet of Things: Connecting Objects*, Wiley Hoboken, New York.

Cisco IBSG., Evans D. (2011), *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [access: 13.08.2015].

Covington M.J., Carskadden R. (2013), *Threat Implications of the Internet of Things*, (in:) Podins K., Stinissen J.M. (Eds.), *NATO CCD COE Publications*, Tallinn, https://ccdcoe.org/cycon/2013/proceedings/d1r1s6_covington.pdf [access: 30.10.2015].

Cruz L. (2014), *London Underground turns to Internet of Things to increase efficiency*, http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1471491 [access: 21.08.2015].

eMarketer (2015), *Internet Users and Penetration Ratio Worldwide 2013-2018*, http://www.emarketer.com/Article/Internet-Hit-3-Billion-Users-2015/1011602, [access: 20.11.2014].

Geer D. (2014), http://www.csoonline.com/article/2134265/network-security/the-internet-of-things--top-five-threats-to-iot-devices.html?page=2 [access: 30.11.2015].

Hess K. (2014), *The Internet of Things outlook for 2014: everything connected and communicating*, http://www.zdnet.com/article/the-internet-of-things-outlook-for-2014-everything-connected-and-communicating/ [access: 10.01.2014].

ITU (2012), *Internet of Things Global Standards Initiative*, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx [access: 13.08.2015].

McKinsey Global Institute (2013), *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute Report May, http://www.mckinsey.com/insights/business_technology/disruptive_technologies [access: 12.08.2015].

Microsoft (2014), *The Internet of Things is helping London Underground run more smoothly*, http://blogs.microsoft.com/firehose/2014/06/06/the-internet-of-things-is-helping-the-london-underground-run-more-smoothly/ [access: 21.08.2015].

Postcapes (2011), *Internet of Things added to the 2011 hype cycle*, http://postscapes.com/internet-of-things-added-to-the-2011-hype-cycle [access: 13.01.2011].

Postcapes (2015), *A brief history of the Internet of Things*, http://postscapes.com/internet-of-things-history [access: 16.08.2015].

Sales Manago & Benhauer Marketing Technologies (2015), *Internet of Things dla marketingowców*, Apayo Brenna, PL.

Shewan D. (2015), *The Internet of Things is already here – and there's nothing you can do about it*, http://www.wordstream.com/blog/ws/2015/01/09/the-internet-of-things [access: 18.11.2015].

Tarabasz A. (2015), *The impact of IoT (Internet of Things) on new approach in network management*, EMNet conference (3-5 December), Cape Town (unpublished materials, conference presentation).

Internet of things – cyfrowa rewolucja na rynku brick & mortar. Szansa czy zagrożenie?

Streszczenie

Zgodnie z prognozami eMarketer, w 2015 roku liczba internautów miała przekroczyć 3,07 miliarda przy współczynniku penetracji tego medium na poziomie 42,4%. Jednocześnie liczba urządzeń mających dostęp do Internetu przekroczy próg 15 miliardów. Co więcej, statystyki te będą gwałtownie rosnąć, ponieważ przewidywana liczba ma przekroczyć poziom 200 miliardów przed końcem 2020 roku. Jednocześnie IoT to nie tylko liczba współpracujących dzięki sieci urządzeń, lecz realna wartość rynku. Szacuje się, iż roczna stopa wzrostu dla *Internet of Things* (IoT) może wahać się od 2,7 na chwilę obecną aż do 6,2 biliona dolarów, przewidywanych w roku 2025. Największy wpływ na te statystyki mają mieć sektor ochrony zdrowia oraz przedsiębiorstwa o charakterze produkcyjnym.

Celem artykułu jest popularyzacja idei IoT (*Internet of Things*), wylistowanie związanych z nią zarówno szans, jak i zagrożeń oraz ukazanie wielkości drzemiącego w niej potencjału. Prowadzone dywagacje będą służyły zobrazowaniu przykładów „inteligentnych rzeczy/urządzeń" (tzw. *smart objects*), sensorów (*sensors*) i lokalizatorów (*locators*); efektywnego procesu zakupowego, które jako całość tworzą zręby inteligentnych zakupów, automatycznych alertów, personalizowanego i/lub inteligentengo opakowania (*personalized, intelligent packaging*) a nawet profilowanej reklamy w VOD (*video on demand*).

Z wymienionych wyżej powodów idea *Internet of Things* wywiera znaczący i niekwestionowany wpływ na zmianę paradygmatu rynku, produktu, oferty, zakresu komunikacji, a także szeroko pojętego biznesowego podejścia do zarządzania firmą. Jednak potwierdza się i w tym wypadku przysłowiowa mądrość, wskazująca, iż „nie ma róży bez kolców". Podobna prawidłowość widoczna jest w przypadku IoT w odniesieniu do licznych cyberataków, w których ze względu na niski poziom bezpieczeństwa posunięto się do przechwytywania, zakłócania, zaprzeczania prawdziwości, pogorszenia, zniszczenia lub manipulacji zasobów zarówno obliczeniowych, jak i informacyjnych. Zdalny dostęp do inteligentnych urządzeń może bowiem prowadzić do potencjalnych wycieków danych wrażliwych (np. informacji zdrowotnej) czy też złośliwych ataków hakerskich ukierunkowywanych zarówno na pracowników niższego szczebla, jak i skierowanych na kluczową kadry kierowniczą w celu wywarcia wpływu lub kontroli stabilności finansowej organizacji. Mając powyższe na uwadze, artykuł nie będzie wyłącznie gloryfikował szeroko rozpowszechnionego pozytywnego podejścia do korzyści możliwych dzięki *Internet of Things*, ale raczej skupi się na zbalansowaniu potencjalnych szans i zagrożeń związanych z opisaną ideą.

Słowa kluczowe: *Internet of Things*, IoT, *smart objects*, *wereables*, konsekwencje innowacji technologicznych, rynek *brick & mortar*, rynek *click & mortar*.

Kody JEL: L86, O33

Internet of things – цифровая революция на рынке brick & mortar. Шанс или угроза?

Резюме

В соответствии с прогнозами eMarketer, в 2015 г. число интернавтов превысило 3,07 млрд. при показателе распространения итого средства на уровне 42,4%. Одновременно число устройств с доступом к интернету превысит порог 15 млрд. Более того, эти статистики будут бурно расти, ибо прогнозное число превысит уровень 200 млрд. до конца 2020 г. Одновременно IoT – это не только число сотрудничающих благодаря сети устройств, но и реальная стоимость рынка. Оценивают, что годовая доля роста для *Internet of Things* (IoT) может колебаться от 2,7 в настоящее время аж до 6,2 биллиона долларов, прогнозируемых на 2025 г. Самое большое влияние на эти статистики должны иметь сектор здравоохранения и производственные предприятия.

Цель статьи – популяризовать идею IoT (*Internet of Things*), указать перечень связанных с ней как шансов, так и угроз, а также указать величину покоящегося в ней потенциала. Проводимые рассуждения послужат для иллюстрации примеров «умных вещей/устройств» (англ. *smart objects*), сенсоров и локализаторов; эффективный закупочный процесс, которые в целом создают костяк умных покупок, автоматических тревожных сигналов, персонализированной и/или умной упаковки, а даже профилированной рекламы в VOD (*video on demand*).

По приведенным выше причинам идея *Internet of Things* содержит в себе значимое и бесспорное влияние на изменение парадигмы рынка, продукта, предложения, сферы коммуникации, а также бизнес-подхода к управлению фирмой в широком смысле. Но и в этом случае подтверждается народная мудрость, указывающая, что «не бывает розы без шипов». Такая же закономерность видна и в случае IoT по отношению к многочисленным кибератакам, в которых из-за низкого уровня безопасности допустились перехвата, глушения, отрицания достоверности, ухудшения, разрушения или манипуляции как рассчетных, так и информационных фондов, ибо удаленный доступ к умнным устройствам может вести к потенциальной утечке чувствительных данных (напр. мединформации) или же к злобным хакерским атакам, направленным как на сотрудников более низкого уровня, так и на ключевых руководящих работников для оказания влияния или контроля за финансовой стабильностью организации. Учитывая вышесказанное, статья не будет исключительно прельщаться широко распространенным положительным подходом к выгодам, возможным благодаря *Internet of Things*, но скорее всего сосредоточится на уравновешении потенциальных шансов и угроз, связанных с описанной идеей.

Ключевые слова: *Internet of Things*, IoT, *smart objects*, «умная» одежда (англ. *wereables*), последствия технологических инноваций, рынок *brick & mortar*, рынок *click & mortar*.

Коды JEL: L86, O33

Artykuł nadesłany do redakcji w lutym 2016 roku

Afiliacja:
dr Anna Tarabasz
Uniwersytet Łódzki
Wydział Zarządzania
Katedra Marketingu
ul. Matejki 22/26
90-237 Łódź
tel.: 42 635 52 05
e-mail: tarabasz@uni.lodz.pl