Uniwersytet
Ekonomiczny
w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 360 · 2018

Zarządzanie 16

Anna Tarabasz

SP Jain School of Global Management in Dubai
anna.tarabasz@spjain.org

CYBERSECURITY AND INTERNET OF THREATS – NEW CHALLENGES IN CUSTOMER BEHAVIOR

Summary: Aim/Purpose – Along with increasing number of Internauts, more and more common practice, especially among the youngest audience, becomes social media oversharing. It means, that sensitive data (identifiable information like birth date, e-mail address, photos, marking location, relationship or marital status, interests, beliefs, and statements signed with own name) is voluntarily revealed by the online users themselves on social networks. At the same time, digital users are exposed to awaiting cyber threats like identity theft, unauthorized access, cyberstalking, cyberbullying, child predators, ransomware, spoofing, snooping, or spying. The main aim of the paper is to showcase the scale of the threat along with emerging solutions. To exemplify such undertaking, case studies of two companies – Du (mobile operator) from United Arab Emirates and mBank (leading retail digital bank) from Poland will be presented, supported with adequate reports on oversharing and cybercrime from the above-mentioned countries, followed with comprehensive description on occurring threats.

Keywords: cyber threat, customer behavior, social oversharing, digital awareness.

JEL Classification: L78, M15, M37.

Introduction

The year 2016 became caesura, as for the first time the penetration rate of Internet users exceeded half of world population, with its number reaching 3,68 billion [InternetWorldStats, 2016]. According to many researchers, along with the trend of stable growth of Internet users, especially among the youngest, a key issue in the field of online security, remains the privacy management [Ulsch, 2014; Symantec, 2015; Trim, Lee, 2016]. With the enormous growth of social networking at Facebook (1.97 billion of users), WhatsApp (1.2 billion), Twitter (320 million), Instagram (600 million), Pinterest and LinkedIn (both 100 million) [Statista, 2016], more and more sensitive data is available online and, importantly, is voluntarily revealed by the users themselves [Smith, 2014; Fereira, 2016; CBOS, 2015; Kupczyk, 2016].

Numerous threats, like identity theft, unauthorized access, cyberstalking, cyberbullying, child predators, ransomware, spoofing, snooping and spying may though occur. With growing number of problems and fears awaiting "Internet of Threats", initially coined Internet of Things devices will soon become relevant to multiple aspects of cyberspace. For this reason, companies shall consider proactive attitude against cybercrime incorporated in focus on educating digital customers in terms of cyber threats and increasing their awareness in this field. Along with the indicated increasing importance of CSR role in communication [Ihlen, Bartlett, May, 2011; McKean, 2014; Visser, Magureanu, Yadav, 2015], with particular emphasis on digital channels [Cohen-Almagor, 2015; Diehl, Karmasin, Mueller, 2016], equally arises the necessity of companies' proactive attitude against cybercrime [Trim, Lee, 2014; Ulsch, 2014] and educating Internet audience about possible threats and changing therefore digital customers' behavior [Paulett, Pinchot, 2012; EDAA, 2013; CBOS, 2015; Wirtualne Media, 2015; Symantec, 2015; Fereira, 2016].

The main aim of this paper is to research the scale of the problem of social media oversharing and define existing cyber threats, along with proposing solutions to overcome them. Therefore, the paper will start with a debrief of the problem arising, followed by multiple juxtapositions and practical examples in order to conclude with solutions emerging.

1. Cybersecurity and Internet of Threats

Numerous threats, like identity theft, unauthorized access, cyberstalking, cyberbullying, child predators, ransomware, spoofing, snooping, and spying are occurring every year and their list is still increasing [Białoskórski, 2012; Gharibi, Shaabi, 2012]. The term "Internet of Threats", coined by Melissa Hathway [Wilczyński, 2017] initially for IOT (Internet of Things) devices, shall be therefore expanded on entire of World Wide Web.

The above mentioned cyber threats are numerous and may refer to the country level of economic development, as well as refer to the end users, resulting from their social media oversharing and equally from online security unawareness. The first type, stated in reference to countries, can be based on vulnerability percentage, spam and network attacks as well on bootnet activity. According to Kaspersky [2018] report, countries the most exposed to detriment and mischief are the furthermost often attacked ones (China, US, Germany, Canada, Argentina, Poland, UK, Australia, Czech Republic, and Finland), though a clear trend network attacks occurring to developing economies is visible (cf. Table 1). These occur on country level and reflect their digital economy preparedness to facing the challenge of hacker attacks. To decrease number of occurrences, very often governmental authorities impose specific law and require implementing centralized solutions from companies. Worth mentioning is the fact, that according to ITU [2017] neither Poland, nor United Arab Emirates (UAE) are top ranked as per cyber security preparedness and stated among the top five: Singapore (GCI Index 0.92), US (0.91), Malaysia (0.89), Oman (0.87), and Estonia (0.84), but having respectively 0.622 and 33rd place for Poland and 0.566 and 47th position.

According to Breach Level Index – BLI [Gemalto, 2017] globally, 1.792 data breaches led to almost 1.4 billion data records compromised worldwide during 2016, an increase of 86% compared to 2015. This may be translated to almost 4 million of records lost or stolen every day; moreover, it gives exactly 2.623 records every minute! Of this compromised data only 4.2% was considered as secure breaches, where encryption introduced made the stolen packages useless.

Identity theft was the leading type of data breach in 2016, accounting for 59% of all data breaches. In addition, 52% of the data breaches in 2016 did not disclose the number of compromised records at the time they were reported. According to the BLI, more than 7 billion data records have been exposed since 2013 when the index began benchmarking publicly disclosed data breaches.

Table 1. Selected cyber threats worldwide by top 10 countries in each category

No.	Vulnerabilities [%]		Spam [%]		Network attacks [%]		Bootnet activity [pcs.]	
	Country	Value	Country	Value	Country	Value	Country	Value
1	China	1.39	United States	17.2	Taiwan	6.64	China	16407
2	United States	1.3	China	14.56	Bangladesh	4.37	United States	2735
3	Germany	1.29	Vietnam	7.20	Venezuela	4.08	South Korea	1109
4	Canada	1.23	India	6.12	Ethiopia	3.22	Russia	621
5	Argentina	1.23	Russia	3.34	Macedonia	3.01	Italy	231
6	Poland	1.22	Germany	3.04	Pakistan	3.00	Japan	130
7	United Kingdom	1.15	Brazil	2.5	South Korea	2.99	United Kingdom	109
8	Australia	1.12	Mexico	1.58	Armenia	2.55	Germany	80
9	Czech Republic	1.11	United Kingdom	1.56	Jordan	2.02	Canada	74
10	Finland	1.10	Spain	1.4	Egypt	2.01	Netherlands	57

Source: Based on: [Kaspersky, 2018].

Across industries, the technology sector globally had the largest amount of data breaches in 2016, summing up to 28%, same as health industry, followed by government breaches (15%).

The healthcare industry accounted for 28% of global data breaches, rising 11% compared to 2015. However, the number of compromised data records in healthcare decreased by 75% since 2015. Education saw a 5% decrease in data breaches between 2015 and 2016, and a drop of 78% in compromised data records. Government accounted for 15% of all data breaches in 2016. However, the number of compromised data records increased 27% from 2015. Financial services companies accounted for 12% of all data breaches, a 23% decline compared to the previous year.

Worth underlining is the fact of lack of awareness in terms of potential threats and educational need in this regard. As rightly indicates Dr. Sameh Aboul-Enein [2017], an Expert Member of the United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, more stress should be put on spreading the awareness among students, government sector employees, and trainings available for the private sector. He claims, that nowadays we should go towards creation a global culture of cybersecurity. To achieve the same, three things need to be simultaneously fulfilled. Firstly, it means creating awareness of the dangers inherent in the abuse of cyberspace. Secondly, it involves all government and corporate organizations should tighten their information management systems and governance to safeguard information security and prevent or at least immediately identify breaches of the system and attempts to tamper with information, and then repair any damage. Thirdly, it includes cybersecurity to become an integral feature of education programmes, ranging from school to university and professional training [Aboul-Enein, 2017].

1.1. Major types of cyber threats and hacktivists

According to dictionary-type definitions as cyber threat, each possibility of a malicious attempt to damage or disrupt a computer network or system shall be considered. However, multiple authors engage with defining such occurrence with different engagement level – from the most personalized and oversimplified one, when attack is perceived from individual's point of view, to the more complex ones, on society or government level. Therefore, using the first approach, "cyber threat (cybercrime) could be defined as attacks designed to target both individuals and organizations (…) in which the malware is planted to entice and individual or an employee (…) to lick on a link embedded in phishing email or at website (..) technology allows a cybercriminal to attach malware via drive-by download, which does not require any links to be clicked" [Chaudry, 2017, p. 78]. Along with the second one, as Brenner [2009] says, it can be defined as probable cybercrime consisting use of computer technology to engage activity that threatens a society's ability to maintain internal order and the level of government may be represented by the US Department of Homeland and Security [ICS-CERT, 2017] cyber threats refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway.

Table 2. Major cyber threats of oversharing in social media or resulting from user online security unawareness

No.	Threat type	Threat description
1	*2*	*3*
1	Botnet	Known equally as zombie army, refers to number of Internet-connected devices used by a botnet owner to perform various tasks. Can be used to perform DDoS (Distributed Denial Of Service). Attacks, stealing data, spam sending, or simply allowing the attacker access to the device and its connection
2	Child predators	Person, very often claiming to be peer, using the Internet with the intention of contacting minors below the age of consent, soliciting sexual relations
3	Cyberbullying	Type of cyber harassment using electronic forms of contact. Increasingly common especially among teenagers. Can be identified by repeated behavior and an intent to harm. Can include posting rumors about a person, threats, sexual remarks, disclose victims' personal information, or pejorative labels
4	Cyberstalking	Use of the Internet or other electronic means to stalk or harass an individual, group, or organization. May include false accusations, defamation, slander, and libel. Often includes monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass, or harass
5	Identity theft	Deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name
6	Phishing	Exploiting fear, anxiety, and system vulnerability urging the unaware users to share their funds. Often combined with stealing passwords, credit card numbers, bank account details, and other sensitive information
7	Ransomware	Subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. Usually based on monetary motive
8	Site compromise	Compromising a social networking site with malicious code, any visitor to the site would be susceptible to attack or simply gathering end-user personal information. Often combined with phishing, like-jacking or link-jacking, in which the last two instead of referring to "like" or redirecting to desired referral, download the malware or infect the device in different manner

Table 2 cont.

1	*2*	*3*
9	Snooping/ Spoofing/ Spying	Snooping (synonymous with sniffing) occurs while login to a website without encryption, with acquiring username and password, equally monitoring the website movement (i.e. capturing the network traffic between affected user and the web). Can mean equally unauthorized access to another person's or company's data, reminding eavesdropping. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device. Spoofing refers to actively introducing network traffic pretending to another person/device. Can refer to data transfer or emails sent. Both snooping and spoofing may be used with spying third party
10	Spam/ malware	Unwanted messages in email inbox. Junk mail advertising is considered rather as annoying and harmless. However, spam messages may contain links, after activation redirect to a website installing malicious software (malware) onto computer
11	Unauthorized access/confidential information leak	Combined with theft, burglary and/or revealing seemingly uncritical technical information to the public

As Gupta, Bhatnagar, and Bhatanagar [2013] rightly say, nowadays the sophistication and complexity of the attacks increases the need for advance anti-malware offerings that appreciate the multiple attack points (web, network, device) used to infiltrate the endpoint and minimize the resources needed to thwart these attacks and protect the asset (equally device and data). Before engaging resources to fight against the occurring cybercrime, one must understand the scale of the threat and its potential types. Josh Fruhlinger [2018], expert from CSO, company providing key insights for enterprise security decision-makers in terms of security disciplines from risk management to network defense to fraud and data loss prevention, rightly notices, that year 2017 was very rough for IT security specialists. Multiple hacktivist top actions like WannaCry, NotPetya, Ethereum, Equifax, or GitHub for sure in subsequent years will find worthy successors. This statement is not at all surprising, having in mind the bargain price needed to be paid for a cyberattack. Bruno Fonseca, Chief Information Security Officer at AXA Gulf, during his presentation on cybersecurity as critical initiative to secure the digital future at DigiTrans 2017 in Dubai was showcasing website with rate card for services of 150.000 skilled hackers from over 140 countries available for hire, starting from $100 per attack with money back guarantee! Offer, presented like in hypermarket, with bundle offer of ransomware as-a-service and DoS attack for free and botnet attack from $2 per hour.

Scale of possible threats, even if expressed in terms of stolen data, lost money or numbers of attacks visualized by Gemalto [2017] (even expressed per second), may not be enough appealing to an average bread eater, until observed live with solutions like Cyber Attack Threats Maps by Kaspersky, Norse or ThreatCloud and briefly described in the above mentioned table (cf. Table 2).

The most astonishing is the fact, that the above-mentioned threats constitute only the proverbial tip of an iceberg, showing the selected intimidations to which Internet users are exposed by hacker's activity. The last mentioned have nothing in common with "home grown computer geeks", but are individuals or create hacktivist groups, having own aims or serving as mercenaries of highly ranked CEOs, CMOs, CTOs, COOs, CFOs, and CIOs. Their real salary remains usually undiscovered, however customers willing to pay for their services may decide to pay flat rate for delivered solution (i.e. Botnet attack – $2/hour or $700 for own one), pay wages, according to needs (starting on hourly rate from $12, average fee oscillating around $20-25, reaching $100 for freelancers). Portals like Pay-Scale state average salary of certified ethical hackers around: $78.000 for Information Security Analyst, $81.000 for Security Engineer, $91.000 for Information Security Engineer, and $94.000 or $109.000 for Information Security Manager. According to researchers from George Washington University [2017], there was high demand for such specialists, with 1 million job posts available, as number of threats is rising exponentially and unfortunately, along with Digital Transformation of companies, the most neglected aspect remains security strategy. Therefore, according to Fidelis [2016] report, particular industries decide to invest more in cybersecurity: 82% growth in telecom, 77% in manufacturing, finance, and healthcare, 71% in retail, 61% in government institutions, and 58% of increase in education sector, in order to prevent the top three threats: malware (viruses, worms, Trojans), phishing and SSL-encrypted ones.

In addition to the above mentioned, according to Hemdal Security [Zahaira, 2016], social media remain favorite hackers' target and in 2016 600.000 accounts on Facebook are being compromised every day, along with social engineering as preferred way to manipulate victims, via accessing from 30 countries, reaching 100 banks, within last two years $1 billion was stolen.

1.2. Data breaches in the UAE and Middle East

According to TrendsMENA [2017], in 2016 approximately 45.2 million Middle East data records were compromised versus global 1.4 billion and over 7 billion of records exposed since 2013, when these statistics started to be cautiously counted. As per the findings of the 2016 Breach Level Index (BLI), released by Gemalto [2017], middle eastern data breaches are up 16.67% in 2016 compared to 2015.

As Mello [2017] says, basing on IBM and Ponemon Institute's research, average cost of a data breach in the Middle East stands at $4.94 million in 2017, indicating a rise of 6.9% since 2016. These breaches cost companies $154.7 per lost or stolen record on average. According to Arabian Marketer [2016] and Arabian Business [2017], UAE tops the list in the Middle East for most employee data leaks with over 15.000 leaked credentials, followed by Saudi Arabia (3.360), Kuwait (203), and Qatar (99). In MENA region, organizations in the technology sector were more exposed than any other, dwarfing employees working in financial services, oil and gas, or chemicals.

According to Gulf News [2017] and results of survey, conducted on behalf of VMWare by Vanson Bourne, revealed that UAE workers expected management to take the blame for security failings even if they were not kept informed of their occurrence. Of the IT decision makers surveyed, 58% expected those at the top to take the blame for a cyberattack despite 36% admitting to not disclosing a significant breach to management. Accordingly, 54% and 37% among office workers admitted they would risk being in breach of their organization's security to carry out their job effectively. Moreover, research findings suggest that many respondents believe cyberattacks are inevitable. Almost two-thirds of those surveyed expected to be hit by a serious attack in the next 90 days and 23% of IT decision makers in the UAE said that cyber threats were moving faster than their defenses. In addition, 40% of IT decision makers said employees who are careless or untrained in cyber security were the greatest security challenge their business faces. According to Rasheed Al Omari (VMware MENA business solutions strategist) [Gulf News, 2017], it shows the disconnection between business leaders and IT decision makers and is symptomatic of the underlying challenge faced as organizations seek to push boundaries, transform, and differentiate as well as secure the business against ever changing threats. Moreover, it clearly proves the urge of challenge in customer behavior – social oversharing and carelessness presented by individuals can be an explosive mixture.

Taking the abovementioned into consideration, as well having in mind the cybersecurity readiness of the region and UAE – listed by ICDL Arabia [2015, 2015/2016, 2017] in its reports, United Arab Emirates hold the third position (with 47th position worldwide, maturing level of readiness, GCI score 0.57 and Federal Law no. 2 on Combating the Cyber Crime), after Oman (4th in Global Rank, mature, 0.87, Royal Decree no. 11/2011) and Qatar (25th, maturing, 0.68, Telecommunications Law no. 34 from 2006), Dubai unveils its Cyber Security Strategy to fight the cyber threats [Gulf News, 2017], based on four pillars of Cyber Smart Society, Innovation, Cyber Security, and Cyber Resilience.

The Cyber Smart Society aims at achieving awareness, skills, and capabilities to manage cybersecurity risks for Dubai's individuals and public and private sectors, therefore encompasses changing the customer behavior part, underlying the basis of this paper.

1.3. Data breaches in Poland

It is difficult to present current data on number of breaches in Poland. Statistics from Symantec [eGospodarka, 2012] out of overall of 556 million of victims of cyberattacks worldwide (which is more than entire population of EU) 7.2 million (out of 38 million of country inhabitants) is yearly impacted in Poland. Losses generated by cyber threats in Poland total for 4.8 billion of PLN (approx. $1.3 billion), with average per victim of 672 PLN (approx. $183). Report revealed, that mobile devices, due to poor patching mechanism, have become the new target of cyber villains, due to the fact, that 2/3 of adults connects to Internet via mobile, which causes twice more threats in comparison to statistics from two years before. Moreover, 34% of surveyed have received on mobile text message from a stranger, inviting to click embedded link or to dial the number to listen to voice message. According to Symantec [eGospodarka, 2012], worldwide 89% of people remove suspicious emails from unknown sender, 83% has at least basic antivirus software and 78% do not open attachments or links in unwanted emails or text messages. Unfortunately, statistics presented in Eurobarometer [2015] 29% of Poles are afraid of their online banking security (as second lowest index among EU member countries, with average of 42% of EU28 countries). 25% are afraid of possibility of abuse of their data online (lowest in entire EU, compared to 43% for EU28), 43% claimed to install antivirus software (2nd lowest in EU versus 61% EU28), 29% are afraid to open email from unknown senders (EU lowest versus 49% EU28), 14% change their passwords on regular basis (EU lowest versus 27% EU28), 17% alternate their password for different services (EU lowest versus 27% EU28) and 8% personalize their security settings (one among lowest in EU versus 18% of EU28). Due to relative low cyber threats awareness, according to Eurobarometer [2015], 19% experienced phishing and online fraud, 22% faced hating, 14% were Internet access-less due to attack, 9% have compromised social media account and been victim of ransomware, 8% experienced identity theft and 43% detected malware on their device.

The biggest hacktivists effects are visible in business approach. According to research by KPF [2016], in 74% of financial institutions faced fraud attempt by using false documents, 37% have been exposed to hackers' attacks, 34% were familiar with skimming or other frauds combined with credit cards use, 34% have noted efforts in overtaking bank account by third party. Equally telecom sector is exposed to similar accounts or data breach, like attack on Netia [Info-Security, 2016], when 14GB of data, including the personal details of customers leaked. But it seems, that government and its institutions are "a tasty morsel" for hackers, wort mentioning are ransomware attack for Polish Defense Ministry with request for $50.000 to be paid in Bitcoins [Das, 2016] or data breach from PESEL system (national identification number system) with more 2 million data compromised, due to access through bailiff's office or compromising governmental Credit Regulation Authority (Komisja Nadzoru Finansowego – KNF), which was used as a gate to hack into systems of multiple commercial banks [O'Neill, 2017].

2. Social oversharing as major transgression

The above-mentioned analysis was showcasing the scale of cybercrime on national level. The fear of unknown and not fully recognized, constitutes a pain point underlying many analysis and awareness campaigns: to protect the existing system against external (and as well internal!) intruders. But the most important point is second type of threats, that refer to individuals' presence on social networking sites, conducing to share almost all kinds of information. This applies to disclosure of sensitive data, especially publication of birth date, e-mail address, photos, marking location, relationship or marital status, interests, beliefs, and statements signed with own name, and is known as social oversharing. The last mentioned, combined with online security unawareness of the Internet users may lead to multiple disastrous consequences.

Research from Kaspersky Lab worldwide [2018] shows that nearly one third of social networking users share their posts, location and multiple private information publicly, not narrowing to friends exclusively. Unaware of enabling accessing this private content, they leave a wide-open door for cybercriminals. With 78% of Internet users having a social networking account, the research reveals clear lack of awareness among users of these sites, as 9% of the participants thought that people outside of their circle of friends would not be able to access their posts and profile. Moreover, increasingly visible becomes trend of unintentionally adding friends to social networking site, with as many as 12% admitting having placed third person to contacts (and friends), regardless knowing it or not. Furthermore, basing on trust for their friends, 26% of the respondents declares willingness of clicking on any link posted by a "friend" from the social networking site. As indicates Smith [2014], even the most developed digital economy in relation to social media, the US, suffers from similar unawareness and equal willingness to share publicly information, that shall not be revealed. But new, more numerous and sophisticated threats are coming. Combining the above-mentioned data, with increasing quality of pictures shared, rises the new opportunities for hackers, as Japan researches already warn on fingerprint theft, resulting from "flashing the peace sign" [AFP, 2017; Harthorne, 2017].

3. Social oversharing in the United Arab Emirates and Poland

With multiple hackers' attacks, which consequences are trying to be minimized, average Internet users "bread eaters" are leaving the door wide open, as if they were inviting them. Not only we use open Wi-Fi, keep using same weak passwords, spot ourselves, open link and download attachments from unfamiliar senders, avoid checking https protocol and install antivirus software. In addition to the above mentioned we overshare, accept unfamiliar contact requests, download applications in favor of email address or mobile phone number.

Despite the sincerest efforts, none of the countries that will be discussed as a case study can be treated as an honorable exception in comparison to the abovementioned US results, as neither Poland, nor the UAE could be treated as leader in not revealing the sensitive data.

According to CBOS [2015], in Poland at least one of the abovementioned information was shared publicly online by 40% of Internet users, and by 71% to some people or companies/institutions. This means that only one-fifth of Internet users (20%) online does not make available any information about themselves and 40% shares something online only with a limited audience. Moreover, in social media almost all Internet users aged 18-24 publish information about themselves publicly and Polish level of security online remains insufficient [Grey Wizard, 2015].

Similar picture reveals study presented by AMEinfo.com [2016] – provider of online business information about the Middle East region. According to this data, in the United Arab Emirates, although 75% of social media users do not interact with people previously added to contacts, yet 49% of respondents accepted 50% of unfamiliar contact requests and 97% have experienced at least one form of cyber assaults. Number of attacks on social media accounts is steadily increasing, with more than one billion reportedly stolen in 2014 and sold online in the black market.

4. Digital campaigns aiming to raise cyber threats awareness

The innovative approach, mentioned by the Author in the introduction, requires focus on educating digital customers in terms of cyber intimidations. Contemporary companies shall though not only meet the market expectations but rather exceed them. The increasing importance of CSR role in communication is often indicated [Ihlen, Bartlett, May, 2011; McKean, 2014; Visser, Magurenau, Yadav, 2015], with particular emphasis on digital channels [Cohen-Almagor, 2015; Diehl, Karmasin, Mueller, 2016]. Equally arises the necessity of companies' proactive attitude against cybercrime [Ulsch, 2014; Trim, Lee, 2016] and educating wider audience about possible threats [Paulett, Pinchot, 2012; CBOS, 2015; Symantec, 2015; Wirtualne Media, 2015; Fereira, 2016; EDAA, 2017].

To face the challenge of arising cyber threats, in parallel shall be conducted activities increasing the security of citizens and campaigns targeted at final customer. That is why, more and more often occur signed treaties and agreements and laws are being imposed. One should mention here, inter alia, the Industry Self-Regulatory Programme in Online Behavioural Advertising (OBA), introduced in Europe, by European Interactive Digital Advertising Alliance [EDAA, 2017] and TRUSTe (data privacy management company). At the same time worth is to recall the Memorandum of Understanding between the TRA (Telecommunication Regulating Authority, 2015) and Dubai Culture, aiming at delivering the safe and secure cyber culture in UAE.

However, as it has been mentioned in prior, the scale of the phenomenon of social oversharing and digital security unawareness, requires systematized approach and unconventional communication, especially from the final customer point of view. To exemplify such undertaking, though, briefly presented will be examples of two companies – Du and mBank.

Du is a mobile operator from United Arab Emirates, that in November 2016 has established a digital campaign "Be Safe", with the hashtag #postwise [Du, 2017]. Shocking material was introduced in a form of creative narratives, based on real-life events, that have happened in the UAE and abroad. It provided targeted audience with a glimpse into the minds of cybercriminals, how they operate, and how seemingly innocent social media posts can spill over into real life and lead to life threatening crimes like kidnapping, child abuse, or burglary.

On the other hand, mBank (leading retail digital bank from Poland) campaign “Nie robisz tego w realu? Nie rób tego w sieci!” [Wirtualne Media, 2015]. The campaign, which title translated means “Do not you do it in real? Do not do it on the net!”, was targeted at people who use banking services on the web: both on computers and smartphones. It aimed [Duszczak, 2015; Grey Wizard, 2015] at increasing the awareness of threats, that banking customers may encounter in the network. Its concept was based on emphasizing the analogy between behaviors in the non-Internet and the web. Bank was willing to underline, that since some security-related behaviors in the real world appeared suspicious, there was no reason to treat them differently on the web.

In relations to occurring multiple cyberattacks, medium preparedness for hacktivists, equally Polish and Emirati governments are trying to increase cyberthreats awareness and prepare their societies for the impact. Admittedly, it is the high time to change the behaviour of Internet users as medium consumers. In vain will be increased companies’ efforts, if awareness of digital average bread eaters is not improved. Although, there are spam filters, nothing will prevent people from clicking on links in emails from unknown senders. Barely anybody scans attachments from trusted business partners and wen file is downloaded and extracted is already too late. Therefore, campaigns on national level shall be supported from parallel bottom-up approach and education from scratch, that is constantly repeated, till it becomes a habit, alternating customer (Internet user) behavior.

Conclusions, recommendations and future scope

Recalling the examples of the campaign described or mentioning government activities resembles just a drop in the sea of needs. However, increasing customer awareness in this regard, shall be supported with any available mean. In relation to the most often occurring mistakes, worth proposing are the solutions emerging (cf. Table 3), equally with the increased presence, especially in digital campaigns.

Table 3. Most often mistakes done online and proposed action plan

No.	Mistake type	Solution emerging
1	Setting too easy password	Using diverse and complex alphanumeric passwords, not related to information publicly available (i.e. birth date), changing them on regular basis
2	Lack of attention on clicking links	Increased awareness on material proposed to read and link to, especially from unknown entities
3	Over trusting open Wi-Fi	Never using public access network to publish on social media, especially any information allowing to track you. Never handling banking transaction with data transfer from unknown source
4	Lack of security in mobile devices	More sensitive data shall be shared with the use of desktop/laptop device, as not always patching the software is equally well done for mobile and wearable devices
5	Lack of awareness on cyber threats	Education on emerging threats, increased awareness
6	Social oversharing	Conscious posting, without assuming, that the privacy settings will protect you. Careful choice of friends and contacts, changing shared information on the basis of targeted audience, clearly defined in prior (family, friends, mates, colleagues, circles of interests, discussion groups, shared publicly)

Multiple cyberattacks occur every year, and as conducted study shows, consumers are not aware enough to understand the importance on prevention against possible threats. Moreover, Internet users willingly exchange various types information for free application, are trustworthy to open Wi-Fi and overshare on social media. Furthermore, they keep repeating the same passwords, avoid using anti-virus software and click eagerly links from untrusted sources, often suffering therefore from phishing or identity theft.

Due to multiple breaches occurring every year and low awareness in terms of cybersecurity among end consumers and their willingness for social media oversharing, further research is required. Future scope is to conduct not only qualitative study based on available literature and case studies, but support with quantitative analysis to determine factors influencing adoption of anti-spyware and increasing the awareness of cyber threats. Another important point to focus future research could be the data privacy policy and General Data Protection Regulation (GDPR), in order not to repeat Facebook Gate and Cambridge Analytica.

Digital campaigns aiming at educating online consumers on the topic of cyber threats may raise as a solution in this difficult situation. Such undertaking, imposed by Du (mobile operator from United Arab Emirates) and mBank (retail digital bank from Poland) constitute examples of good practice in this regard. Corporate Social Responsibility (CSR) in this aspect shall not only become factor of competitive advantage in branding and positioning, but rather contribute to business ethics and responsible management. This approach requires focus on educating digital customers and therefore step-by-step change of habits in customer behaviour in terms of cyber threats and proactive attitude, as prevention is better than cure.

References

Aboul-Enein S. (2017), *Cybersecurity Challenges in the Middle East*, Centre for Security Policy, Geneva, pp. 1-52.

AFP (2017), *Japan Researchers Warn on Fingerprint Theft from 'Peace' Sign*, retrieved from: https://www.yahoo.com/tech/japan-researchers-warn-fingerprint-theft-peace-sign-101451701.html (accessed: 10.11.2017).

AMEinfo (2016), *Cybercrime Alert: Nearly Half of UAE Users Add People They Don't Know*, retrieved from: http://ameinfo.com/technology/it/social-media-facebook-cyber-threat/ (accessed: 15.11.2017).

Arabian Business (2017), *UAE is Most at Risk for Employee Data Leaks in the Middle East*, retrieved from: http://www.arabianbusiness.com/uae-is-most-at-risk-for-employee-data-leaks-in-middle-east-647029.html (accessed: 4.12.2017).

Arabian Marketer (2016), *UAE Tops Middle East List for Most Employee Data Leaks: Report*, retrieved from: https://arabianmarketer.ae/uae-tops-middle-east-list-for-most-employee-data-leaks-report/ (accessed: 20.12.2017).

Białoskórski R. (2012), *Cyberthreats in the Security Environment of the 21st Century: Attempt of the Conceptual Analysis*, "Journal of Security & Sustainability Issues", Vol. 1 (4), pp. 249-260.

Brenner S. (2009), *Cyber Threats The Emerging Fault Lines of the Nation State*, Oxford University Press, New York.

CBOS (2015), *Bezpieczeństwo w Internecie*, CBOS report 109/2015, Centrum Badania Opinii Społecznej, Warszawa.

Chaudry P. (2017), *The Looming Shadow of Illicit Trade on the Internet*, "Business Horizons", Vol. 60, pp. 77-89.

Cohen-Almagor R. (2015), *Confronting the Internet's Dark Side. Moral and Social Responsibility on the Free Highway*, Cambridge University Press, New York.

Das S. (2016), *Hackers Attempt to Extort Polish Defense Ministry for $50,000 in Bitcoin*, retrieved from: https://hacked.com/hackers-attempt-extort-polish-defense-ministry-50000-bitcoin/ (accessed: 20.11.2017).

Diehl S., Karmasin M., Mueller B. (2016), *Handbook of Integrated CSR Communication*, Springer, New York.

Du (2017), *Be Safe*, retrieved from: http://www.du.ae/personal/helpandsupport/mobile/besafe (accessed: 10.11.2017).

Duszczak P. (2015), *Internetowe grzechy Polaków*, retrieved from: http://www.network magazyn.pl/internetowe_grzechy_polakow (accessed: 15.11.2017).

EDAA (2017), *Truste/EDAA Research Shows Digital Advertising Self-Regulatory Programme Continues to Improve Consumer Attitudes Towards Interest-based Advertising*, retrieved from: http://www.edaa.eu/edaa-news/truste-edaa-research-shows-digital-advertising-self-regulatory-programme-continues-to-improve-consumer-attitudes-towards-interest-based-advertising/ (accessed: 10.11.2017).

eGospodarka (2012), *Symantec – cyberprzestępczość 2012*, retrieved from: http://www.egospodarka.pl/85789,Symantec-cyberprzestepczosc-2012,1,12,1.html (accessed: 15.05.2017).

Eurobarometer (2015), *EU Special Report Report (423) on Cyber Security*, retrieved from: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf (accessed 15.03.2018).

Fereira O. (2016), *The Dangers of Social Media and Oversharing*, retrieved from: http://singlegadget.com/the-dangers-of-social-media-and-oversharing/ (accessed: 30.11.2017).

Fidelis (2016), *CyberEdge Group: 2016 Cyberthreat Defense Report*, retrieved from: https://www.fidelissecurity.com/resources/cyberedge-group-2016-cyberthreat-defense-report-0 (accessed: 20.11.2017).

Fruhlinger J. (2018), *What is a Cyber Attack? Recent Examples Show Disturbing Trends*, retrieved from: https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html (accessed: 9.03.2018).

Gemalto (2017), *Breach Level Index*, retrieved from: http://breachlevelindex.com/data-breach-database.php?range=2016 (accessed: 30.11.2017).

George Washington University (2017), *Cybersecurity by the Numbers*, retrieved from https://security.online.gwu.edu/blog/cybersecurity-by-the-numbers (accessed: 15.10. 2017).

Gharibi W., Shaabi M. (2012), *Cyber Threats in Social Networking Websites*, "International Journal of Distributed and Parallel Systems (IJDPS)", Vol. 3, No. 1, pp. 119-126.

Grey Wizard (2015), *Internetowe grzechy Polaków*, retrieved from: https://infowire.pl /generic/release/303737/internetowe-grzechy-polakow/ (accessed: 30.11.2017).

Gulf News (2017), *Dubai Unveils Strategy to Fight Cyber Threats*, retrieved from: http://gulfnews.com/news/uae/government/dubai-unveils-strategy-to-fight-cyber-threats-1.2036181 (accessed: 9.05.2018).

Gupta N., Bhatnagar A., Bhatanagar J. (2013), *Cyberpreneur's Wake-up Call: Cyber Security and Millennial Talent Crisises*, Richard Ivey School of Business Foundation, HBR W13439-HCB-ENG, pp. 1-7.

Harthorne M. (2017), *Flashing the Peace Sign Can Get your Identity Stolen*, retrieved from: http://www.foxnews.com/tech/2017/01/12/flashing-peace-sign-can-get-your-identity-stolen.html (accessed: 30.11.2017).

ICDL Arabia (2015), *Cyber Safety Report. Research into the Online Behavior of Arab Youth and Risks They Face*. ICDL Arabia, Dubai, pp. 3-34.

ICDL Arabia (2015/2016), *Social Media: Influencing Young Minds*, ICDL Arabia, Dubai, pp. 2-37.

ICDL Arabia (2017), *Cyber Readiness Report 2017-2018. How ready is the GCC Region with Cybersecurity?* ICDL Arabia, Dubai, pp. 3-38.

ICS-CERT (2017), *Cyber Threat Source Descriptions*, retrieved from: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (accessed: 3.12.2017).

Ihlen Ø., Bartlett J., May S. (2011), *The Handbook of Communication and Corporate Social Responsibility*, Wiley-Blackwell, Hoboken.

InfoSecurity (2016), *Polish Telco Netia Suffers Major Breach*, retrieved from: https://www.infosecurity-magazine.com/news/polish-telco-netia-suffers-major/ (accessed: 20.11.2018).

InternetWorldStats (2016), *World Internet Users and 2016 Population Stats*, retrieved from: http://www.internetworldstats.com/stats.htm (accessed: 30.11.2017).

ITU (2017), *Global Security Index Report (2017)*, electronic version, pp. 1-47.

Kaspersky (2018), *Cybethreat Statistics*, retrieved from: https://cybermap.kaspersky.com/stats// (accessed: 22.11.2018).

Konferencja Przedsiębiorstw Finansowych w Polsce [KPF] (2016), *Cyberprzestępczość rosnącym problemem*, retrieved from: https://kpf.pl/badanie-kpf-i-ey-cyber przestepczosc-rosnacym-problemem-co-trzecia-instytucja-finansowa-spotkala-sie-z-tym-typem-naduzycia/ (accessed: 25.11.2017).

Kupczyk P. (2016), *Użytkownicy nie dbają o prywatność na portalach społecznościowych*, retrieved from: http://di.com.pl/uzytkownicy-nie-dbaja-o-prywatnosc-na-portalach-spolecznosciowych-54106 (accessed: 13.12.2018).

McKean J.S. (2014), *Customer's New Voice: Extreme Relevancy and Experience Through Volunteered Customer Information*, John Wiley & Sons, Hoboken.

Mello S. (2017), *Why Data Security is Key for UAE Firms*, retrieved from: https://www.khaleejtimes.com/technology/why-data-security-is-key-for-uae-firms (accessed: 12.11.2017).

O'Neill P. (2017), *Hackers Break into Polish Banks through Government Regulator Charged with Bank Security Standards*, retrieved from: https://www.cyberscoop.com/hackers-break-polish-banks-government-regulator-charged-bank-security-standards/ (accessed: 25.01.2018).

Paulett K., Pinchot J. (2012), *Cybercrime: The Unintentional Effects of Oversharing Information on Facebook*, Proceedings of the Conference on Information Systems Applied Research, Vol. 5, pp. 1-7. New Orleans.

Smith A. (2014), *Half of Online Americans Don't Know What a Privacy Policy is*, retrieved from: http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is (accessed: 30.11.2017).

Statista (2016), *Countries with the Highest Commitment to Cyber Security Based on the Global Cybersecurity Index (GCI) as of September 2016*, retrieved from: https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/ (accessed: 30.11.2017).

Symantec (2015), *Internet Security Threat Report*, retrieved from: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf (accessed: 20.11.2017).

TrendsMENA (2017), *16.67% More Middle East Data Breaches in 2016 Compared to 2015*, retrieved from: https://trendsmena.com/management-marketing/16-67-middle-east-data-breaches-2016-compared-2015 (accessed: 25.09.2017).

Trim P., Lee Y. (2016), *Cyber Security Management. A Governance, Risk and Compliance Framework*, Routledge, New York.

Ulsch M. (2014), *Cyber Threat! How to Manage the Growing Risk of Cyberattacks*, John Wiley & Sons, Hoboken.

Visser W., Magureanu I., Yadav K. (2015), *The CSR International Research Compendium*, Kaleidoscope Futures, London.

Wilczyński Ł. (2017), *Cyberbezpieczeństwo oraz Internet Zagrożeń – nowe wyzwania dla specjalistów ds. komunikacji*, retrieved from: http://nowymarketing.pl/a/16460, cyberbezpieczenstwo-oraz-internet-zagrozen-nowe-wyzwania-dla-specjalistow-ds-komunikacji (accessed: 30.11.2017).

Wirtualne Media (2015), *Nie robisz tego w realu? Nie rób tego w sieci!*, retrieved from: http://www.wirtualnemedia.pl/artykul/nie-robisz-tego-w-realu-nie-rob-tego-w-sieci-mbank-ostrzega-przed-zagrozeniami-w-internecie-wideo (accessed: 30.11.2017).

Zahaira A. (2016), *10 Alarming Cyber Security Facts that Threaten Your Data*, retrieved from: https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/ (accessed: 25.11.2017).

CYBERBEZPIECZEŃSTWO I INTERNET ZAGROŻEŃ – NOWE WYZWANIA W ZACHOWANIU KLIENTÓW

Streszczenie: Wraz z rosnącą liczbą użytkowników Internetu coraz powszechniejszą praktyką, szczególnie wśród najmłodszych odbiorców, staje się social media oversharing, czyli nadmierne upublicznianie treści w ramach mediów społecznościowych. Oznacza to, że wrażliwe dane (identyfikowalne informacje, takie jak: data urodzenia, adres e-mail, prywatne zdjęcia, oznaczenie lokalizacji, status związku lub stan cywilny, zainteresowania, przekonania czy też oświadczenia podpisane własnym nazwiskiem) są dobrowolnie ujawniane przez użytkowników. Jednocześnie są oni narażeni na czyhające zagrożenia cybernetyczne, takie jak: kradzież tożsamości, nieautoryzowany dostęp, nękanie, cyberprzemoc, zagrożenia pedofilią, oprogramowaniem wymuszającym okup, podszywanie się i szpiegowanie. Głównym celem artykułu jest przedstawienie skali zagrożenia wraz z prezentacją dostępnych rozwiązań i przeciwdziałań. Jako przykład takiego przedsięwzięcia zostaną przedstawione studia przypadków dwóch firm – Du (operatora telefonii komórkowej ze Zjednoczonych Emiratów Arabskich) oraz mBanku (wiodącego cyfrowego banku detalicznego z Polski), poparte odpowiednimi raportami na temat oversharingu i cyberprzestępczości z wyżej wymienionych krajów.

Słowa kluczowe: cyberzagrożenie, zachowanie konsumentów, cyfrowa dojrzałość, social media oversharing, cybernarcyzm.