Cyberattacks and their impact on online brands' image

A kibertámadások és hatásuk az online márkák imázsára

AUGUSTYN, Duszan Józef[1]

Abstract

The development of cyber-economy is creating new threats for brands and their public relations, especially for companies from sectors of online services and IT. Outcomes of cyberattacks are the new types of PR challenges for companies that can negatively impact a brand's image, reliance on products and services provided, and lead to general distrust towards whole branches of cyber-economy. Brands providing services related to online services or IT are especially vulnerable to the marketing consequences of cyberthreats. Online services are using personal data and financial assets of the users which may be intercepted, leaked out, stolen, misused, modified, replaced, and be used against the user's will or interest. In this regard, brands must prepare defense strategies from cyberattacks together with plans for dealing with the negative outcomes of cyberattacks and their consequences for the brand. This paper will focus on the threats for brand image related to cybersecurity, potential impacts of cyberattacks on user's perception of brand trust towards it, and how the companies may secure their customers and react to cyberattacks on them.

Keywords

Cyberbranding, cybertrust, PR, online security, online brands, brand trust, ICT-security, data protection

Absztrakt

A kibergazdaság fejlődése új fenyegetéseket jelent a márkák és azok közönségkapcsolatai számára, különösen az online szolgáltatásokra és az informatikai szektor vállalkozásaira nézve. A kibertámadások új PR-kihívásokat jelentenek a vállalatok számára, melyek negatívan befolyásolhatják a márka imázsát, és csökkenthetik a kínált termékekbe és szolgáltatásokba vetett bizalmat. Az online és informatikai szolgáltatásokkal kapcsolatos márkák különösen kiszolgáltatottak a kiberfenyegetések marketingre gyakorolt hatásaival szemben. Az online szolgáltatások a felhasználók személyes adatait és pénzügyi eszközeit használják, melyeket kibertámadások során lehallgathatnak, kiszivárogtathatnak, ellophatnak, és a felhasználó akarata vagy érdeke ellenére használhatnak fel. E tekintetben a márkáknak védelmi stratégiákat kell kidolgozniuk a kibertámadások ellen, valamint terveket készíteni a kibertámadások márkára gyakorolt negatív következményeinek kezelésére. Jelen tanulmány a márkák imázsának kiberbiztonsággal kapcsolatos fenyegetéseire összpontosít, és a kibertámadások lehetséges hatásait vizsgálja a márka iránti bizalomra. Továbbá arra keresi a választ, hogy a vállalatok hogyan biztosíthatják ügyfeleiket, és hogyan reagálhatnak az őket ért kibertámadásokra.

Kulcsszavak

Kibermárka, kiberbizalom, PR, online biztonság, online márkák, márkabizalom, IKT-biztonság, adatvédelem

[1] mail@duszan.pl | ORCID 0000-0002-3291-9930 | Kutató a krakkói Jagelló Egyetemen | Researcher at Jagiellonian University in Kraków

INTRODUCTION

Few key brand features are essential for brand success. Trust (Kim & Benbasat, 2003) among security and privacy (Reedy, Schullo, & Zimmerman, 2000). Trust is associated with the features of the brand like logo, message, values, products, and services provided under the brand's name. One of the attributes of brand success in IT and online services is a cyber-branding strategy (Breakenridge, 2001).

It is a keystone for companies from the IT and online services sector to build secure and trusted services for their users, to develop procedures to actively defend and protect their systems, but as well to prepare mechanisms allowing them to cope with brand crises where safety, privacy, and assets of customers are endangered. For that IT and online services brands have not only to prepare effective reaction schemes towards critical cybersecurity hazards but as well they must create a way to keep the customer trust towards their brands even after significant damage caused by vulnerability of service ICT-Security. Because of the specificity of the dynamically changing and impersonal character of IT and online services sectors it may be much more challenging to keep the customer's trust than for traditional brands based on physical products or services provided or sold by a physical person.

DEFINITION OF BRAND

A brand is a set of features that are identifying and distinguishing a good or service from others. Brands can have features as name, design, symbol, or other brand-attributes fulfilling this requirement (Kotler & Armstrong, 1994). Taking into account the aspect of benefits for consumers, a brand is a set of functional and symbolic elements allowing to build a loyal group of consumers, and enable the brand owner to achieve a leading position in the market by fulfilling the marketing strategies of the company (Ghodeswar, 2008).

A brand can consist of verbal (name) and non-verbal (symbol, logo) elements. A brand may include the associations to names of cities, countries, and regions, names of animals, symbolizing nature (Edwards & Day, 2005). Names can come from history, pop culture from literary and musical works. The brand can consist of combinations of letters, digits, or symbols. The brand or part of the brand protected by law becomes a trademark and that may be used only by the brand owner and cannot be copied or imitated.

An attempt to systematize consumer behavior concerning online brands was made by G. Shao. According to his view, these behaviors include consumption, co-participation, and creation of content concerning brands (Shao, 2009). This approach was developed and detailed in D.G. Muntinga et al. research, which resulted in the definition of a framework for online consumer activity concerning brands. Depending on the degree of consumer involvement, they distinguish three types of such activity: consumption, contribution, and creation (Mutinga, Moorman, & Smit, 2011).

IT and online brands have the lowest level of consumer involvement in brand activities is consumption. It is the most common type of behavior that is related to the fact that it requires only the passive reception of the content related to a specific brand, placed on the Internet by other Internet users or brand owners. Examples of this type of action include watching videos, reviewing ratings, comments, and opinions on brands and reading discussions on brands on social networking sites (Schivinski & Brzozowska-Woś, 2015).

A higher level of involvement in consumer's online brand-related activities is characterized by the contributory type. Consumers contribute to the creation of brand-related content by participating in brand discussions on fan sites, writing comments on brands, or adding content e.g. photos, graphic messages, and videos on blogs and fan pages.

The highest level of consumer activity on the Internet concerning brands is the creative type of consumer's online brand-related activities. Examples of this type of behavior include running blogs devoted to particular brands, publishing product reviews, and creating and placing on the Internet e.g. films, photos, graphic messages, sound files related to a brand. This means that consumers representing the creative type are the creators of branded content that will later be consumed or contributed to by others.

IMPACT OF TRUST ON BRANDS

Trust has an impact on an online consumer's devotion to the brand. D. A. Aaker is defining brand quality as the consumer's perception of the overall quality of a product or service, or their superiority compared to alternative products and services. This hard to grasp feeling towards the brand, based on brand-related product or service characteristics such as reliability and performance (Aaker & Joachimsthaler, 2000), is impacting the perception of trust towards the brand. A brand may be associated with trust towards its features, but as well through the experience that is promising, or by the quality of the service or product that the company delivered to the customer before, building a positive association with the brand (Kotler, 2006).

The concept of trust is interpreted in terms of:

- Disposition - i.e. a mental subjective attitude towards the brand (evaluation, anticipation, expectation)
- Decision – extrapolated reliance on the product or service, a user is allowing itself to be dependent on the brand
- Behavior – a physical emanation of trust towards the brand.

Trust is an important resource of the organization and may be considered as the starting point for many management concepts. Trust management is a set of activities to create systems and methods, which allow dependent entities to make assessments and undertake decisions on the reliability of risky activities, as well as to enable these entities to develop and use brand credibility as their own. (Grudzewski, Hejduk, Sankowska, & Wańtuchowicz, 2009)

Trust in the brand can be categorised as consumer risk. The lower the expected and perceived risks the greater the confidence the consumer can give the brand. The most common risks that the consumers are taking:

- Performance - to what extent the brand is consistent with the description of the functions it performs.
- Financial - whether the brand will provide the right value for money spent (price).
- Time - does the consumer need to spend more time assessing the unknown of brands, and if the brand is unsuitable, how much time is left wasted.
- Social - whether the brand will be accepted by family, friends and whether
- the purchase will change their opinion about the buyer.

- Psychological - whether the consumer feels well as a brand owner (De Chernatony & McDonald, 2003).

INSIGHT ON BRANDS IN IT AND ONLINE SERVICES SECTOR

Trust plays an important role in the customer decision-making process in accordance with the will to undertake an economic activity, register, leave personal and financial data, and being tracked or monitored by data administrators. It is proven that business operations may be done more effectively if there is a customer trust towards the brand (Zucker, 1986). In the dynamic and competitive online services markets where the distance or time of realization of services has no impact or lower impact than in other spheres of economy, trust towards the brand may be the only assurance that the customer can have towards the enterprise. Because of lack of personal contact with the customer service and obligation of tracking support requests, is creating an atmosphere where the trust is associated only with the brand or product, and not as in traditional customer service with a physical company representative or salesman. Many online companies are having non-direct customer service which is not encouraging them to use it for help or complain as a traditional one for many users.

Lack of trust towards the brand is the key reason why people do not make purchases online (Lee & Turban, 2001). Security is among others considered as one of the important determinants and core elements of the online trust (Dayal, Landesberg, & Zeisser, 1999). Therefore, the brand manager must consider trust in the brand as a key asset of the marketing strategy. In this context, strong and trustful online brands can take the role of a consumer guide for those who are not keeping pace with rapid technological change, marketing confusion, and information noise on the market. In the multitude of information and opinions on the various offers available, offers marked with a strong brand increase confidence in the customer decision to purchase (Urbanek, 2008).

DEFINITION AND CATEGORIZATION OF CYBERTHREATS

There are several security threats impacting a brand’s name and they may be divided into three levels:

- Allowing external users to access the system in an unauthorized way.
- Allowing users to have more rights and access to the platform than it was planned within the system.
- Events or actions that are affecting users’ service quality on the platform, causing stoppages delays or leading to a system interruption.

Breach of every security risk level is a threat to the platform stability (Alhabeeb, Almuhaideb, Le, & Srinivasan, 2010) and can negatively impact the users’ trust concerning the brand. Several aspects of users security or platform stability may be a subject of risk that can impact the brand’s reputation:

- Personal data and user history (Zhang, 2014).
- Financial assets security.
- Anonymity of information (Medaglia & Serbanati, 2010).
- Service quality.
- Misleading of users, miscommunication, or lack of communication (Weber, 2010).

Security risk and security threats may have short term consequences (related to user satisfaction) and long term consequences (related to PR of the brand) connected with the stability of the platform and company and the brands' reputation. It is crucial for the companies to prevent the security risks because once the website would be classified as a potential danger by search engines, antiviruses or other applications responsible for the online security for the users, it is hard to rebuild the trust of users and categorization by search engines' algorithms.

There may be some preventive measures to avoid the emergence of the security threats (Gerić & Hutinski, 2007) such as software-based security measures (Barabanov, Markov, & Tsirlov, 2018), hardware-based security measures (Al-Omary, Othman, AlSabbagh, & Al-Rizzo, 2018) and user-based security measures (Toršić, 2018).

FACTORS OF CYBER-THREATS ON IT AND ONLINE SERVICES BRANDS PERCEPTION

External factors of the online service perception such as different markets, cultures or legislation are impacting the trust towards the service (Doney & Cannon, 1997). The other factors related directly to the IT and online services are:

- Consumer characteristics.
- Past user experience with the service or other online services.
- Perception of risk of using a service or a specific type of service
- Trustworthiness towards the service.
- The reputation of the brand.
- Website quality.
- Perceived usefulness of the service for the user.
- Perceived ease of use of service.
- Familiarity with the interface.
- Trusted seal given by the external authority.
- Experts opinion.
- Peers' opinion.
- Non-government or non-business association.

Factors impacting users' perception of safety are significant elements of acquiring trust towards an online brand. (Shah Alam & Mohd Yasin, 2010) The stronger is the perceived quality of service and brand safety, the higher is the level of trust towards the brand.

IT AND ONLINE BRANDS DAMAGE CONTROL STRATEGIES

Companies may deal with the negative reputation of their brands through several direct and indirect methods. The key aspect of those actions is to not let the bad reputation spread, and to reduce the sprawl of the information out of the bubble of customers who were already impacted by losing the security risk. The other aspect is to prevent the bad reputation to reach the new customers and Internet users who have not yet decided if they want to use the service or which service provider to use.

The damage control strategies used by brand managers may be:

- Fixing the reason for the distrust – to stop the proliferation of the security risk and to not expose other users of the Internet to the risk. The other way is to avoid escalation of negative word of mouth directed to the brand, especially with the use of social media and other activities associated with the service.
- Removal of negative reviews about the brand – to minimize the impact of negative reviews and opinions on the brand impacting current and new users of the service. This activity may be overcommitted by a brand manager and look as fake from the perspective of the user, because of that, the situation when service has no opinions or no reviews at all has to be avoided.
- Removal of negative message about the brand portraying it as dishonest – one of the worst images for the brand is to denude company profit orientation to the customers or present itself as non-interested in solving issues related to customer losses. In many situations, the way of conduct of the representatives of the brand or customer service agents may be considered by users as not empathetic, not proactive enough, or read as an approach without commitment to solving the customer problems. In some cases, it may be perceived as greedy and profit-oriented, especially when the fault of malfunction or cyber-risk is not on the user side or it is not perceived as such.
- Add positive opinions and reviews – users are expecting confirmation and assurance of the brand's professionalism and safety. One of the ways that users are looking for confirmation of such aspects is looking for active and independent opinions of users validating customer expectations related to a brand. Some companies are faking user opinions which may be revealed by users. In this situation, the outcome of such a move may bring contradictory effects to ones desired.
- Satisfying users who were impacted by the negative event – users who lost their assets or were stressed by the gap in company security systems are generally expecting a satisfaction of their loss. Dissatisfied customers may tend to spread negative information into the general public and by word of mouth. Giving the dissatisfied user extra gratification may reduce the frustration directed towards the brand and prove the company's professional and customer-oriented approach towards customer service. In some cases, customers may appreciate the satisfaction given and consider the risk-related situation as an accident that happened only once and it will not occur again, and the users may stay loyal to the brand.
- The distraction of haters of the brand – if the brand will gain its group of haters whose goal will be to disregard the brand in the public of Internet (doesn't matter if they are appearing as an effect of company mismanagement and policies or haters steered by the competition), the most efficient way to deal with hate towards the brand is to distract the haters. Distraction may be done by making haters' efforts insignificant and it may be achieved through focusing their complaints to not essential elements of the issue or to reveal the hating intentions or association with competitions of haters. Revealing intended hate initiated by competition may turn into a positive reaction of sympathy towards the brand.

- Providing an excellent level of customer service – customer service is a must when speaking about a successful brand image. In a situation of crisis, the behaviour of customer service agents or brand representatives is crucial for the brand's reputation. In the situation when service is working properly, for many users a brand is a seemingly invisible feature of product or service. The emotion tied with the realization of the brand is occurring during hurdles and in this particular situation, customer service is an indicator of the professionalism of the service.
- Preclusion of usage of the incident by competitors – in the competitive market competitors may seek easy gain by diminishing the market position of the company by utilizing the issues related to security. Crisis security situations may lead to the outflow of customers so it is important to manage to keep them associated with the brand and provide them a vision of better service quality despite the troubles caused to them before. There are reasons why users prefer to stay with brands and services that they are already used to like: familiar interface, already configured account, access to the history of service usage, networking build-up though the service, discounts collected by the time of usage of the service, gamification of service design and sympathy for the brand. A brand manager has to use it to minimize the users' outflow or general disappointment with the usage of this type of online service.
- Rebranding – in the situation when the damage given to the brand is too heavy for it to recover from. There may be a need to rebrand the brand's elements or to drop it down totally. One of the ways how companies may use rebranding is changing its association with particular elements and messages used by brands to communicate certain features to the customers. Rebranding may be directed into strengthening the weak points of current brand strategy or to distract users with a new stronger message that will have a goal to associate the brand with.
- Positive employer branding – in the case of some businesses, its employees or associates are numerous they may be a significant marketing asset. On the other hand, every employee may be a potential threat of an unauthorized leak of information or a cause of an inside job. A positive company branding may make company workers proud to work for the brand and by that, they become defenders of the brand's name and work for the brand as it is directly associated with them.
- Corporate Social Responsibility – strategy of corporate social responsibility may work as a long term strategy and it may be considered more as a strategy to build-up the brand than to use it in the crisis. But there are some situations where CSR may help to reach certain customer groups or to be used for users particularly devoted to certain values or concerns that the CSR strategy may answer.

CONCLUSION

Online and IT brands operating in a competitive environment, filled with potential security risks have to acquire user's trust to effectively gain and keep their customers. A high level of the ICT-security of the online platform is a key value that companies have to deliver, therefore the perception of trust is one of the most important features that have to be associated with a trustful brand. In the situation of crisis brands are the most vulnerable asset of the company related to the potential loss of users and decrease of reputation leading to marginalization on the market. To inhibit this process brand managers have to prepare strategies that are allowing the service to deal with the crisis before the cyber-threats appear and to have prepared procedures and ways of conduct on the situation after the cyber-threat would emerge.

There are several ways to make the brand proof of security incidents and to cope with the negative image caused by it. Trust towards the brand is valuable not only during the time of crisis but it has to be build-up and grow together with user familiarization with it and during the time of interaction with it. The stronger the level of trust is created the more crisis-proof it becomes.

It is possible to distinguish the direct and indirect ways to cope with the security incidents relating to the trust of the brand, all of them require active reaction from the brand manager and whole service to minimize the damage caused by the security incident. A brand is the simplified emanation of user's perception of the service and it has to reach their expectations towards it. On the other hand, a brand cannot be detached from the service and its functionalities, therefore all the channels of building the customers experience related to the brand (service quality, service architecture, customer service, brand image) have to be integrated into one coherent vision and have to be included in the brand strategy. In this regard, from the perspective of the company not only the brand manager takes care of the brand's image, but all of the project associates will be familiarized with the brand strategy, its features, and the message that is willing to deliver to the customer. During the security incident brand managers have to closely cooperate with the customer service, financial and technical department in order to avoid unnecessary PR occurrences and lead the brand through the crisis with the least damage possible.

REFERENCES

[1] A. Al-Omary, A. Othman, H. M. AlSabbagh and H. Al-Rizzo, "Survey of Hardware-based Security support for IoT/CPS Systems," in Sustainability and Resilience Conference: Mitigating Risks and Emergency Planning, Amway, 2018.

[2] A. H. Keyhanipour, B. Moshri, M. Kazemian, M. Piroozmand and C. Lucas, "Aggregation of web search engines based on users' preferences in WebFusion," Knowledge-Based Systems vol. 20, pp. 321-328, 2007.

[3] A. Madhavi and K. Harisha Chari, "Architecture Based Study Of Search Engines And Meta Search Engines For Information Retrieval," International Journal of Engineering Research & Technology (IJERT) vol. 2 issue 5, pp. 1832-1835, 2013.

[4] A. V. Barabanov, A. S. Markov and V. L. Tsirlov, "Information Security Controls against Cross-Site Request Forgery Attacks on Software Applications of Automated Systems," in International Conference Information Technologies in Business and Industry 2018, Tomsk, 2018.

[5] B. M. Ghodeswar, „Building brand identity in competitive markets: a conceptual model," Journal of Product & Brand Management Volume 17 Issue 1, 2008.

[6] B. Schivinski and W. Brzozowska-Woś, "Badanie aktywności online polskich konsumentów dotyczącej marek," e-mentor nr 2(59, p. 77–85, 2015.

[7] C. G. Bell and A. Newell, Computer Structures: Readings and Examples, New York: McGraw–Hill Book Company, 1971.

[8] C. M. Medaglia and A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," the Internet of Things, pp. 389-395, 2010.
[9] D. A. Aaker and E. Joachimsthaler, Brand leadership. Building assets in an information economy, 2000: The Free Press, New York.
[10] D. Breakenridge, „Brand Building in The Digital Economy," w Cyberbranding, Upper Saddle River, Prentice Hall, 2001.
[11] D. G. Mutinga, M. Moorman and E. G. Smit, "Introducing COBRAs: Exploring motivations for brand-related social media use," International Journal of Advertising Vol. 30, No. 1, pp. 13-46, 2011.
[12] D. Kim and I. Benbasat, "Trust-related arguments in Internet stores: a framework for evaluation," Journal of Electronic Commerce Research, vol. 4, no. 2,, pp. 49-64, 2003.
[13] E. W. Felten, D. Balfanz, D. Dean and D. S. Wallach, "Web Spoofing: An Internet Con Game," Technical Report 540–96, pp. 1-9, 1997.
[14] G. Shao, „Understanding the appeal of user-generated media: A uses and gratification perspective," Internet Research Vol. 19, No. 1, pp. 7-25, 2009.
[15] G. Urbanek, „Strategie zarządzania aktywami niematerialnymi przedsiebiorstwa," Przegląd organizacji, pp. 13-16, 6 2008.
[16] H. Edwards and D. Day, Creating Passion Brands, London: Kogan Page, 2005.
[17] J. Reedy, S. Schullo and K. Zimmerman, Electronic Marketing: Integrating Electronic Resources into the Marketing Process, Mason: The Dryden Press, 2000.
[18] L. De Chernatony and M. McDonald, Creating Powerful Brands in Consumer, Service and Industrial Markets, Oxford: Elsevier/Butterworth-Heinemann, 2003.
[19] L. Erdödi, N. Ulltveit-Moe, H. Nergaard, T. Gjøsæter, E. Kolstad and P. Berg, "Secure Information Sharing in an Industrial Internet of Things," arXiv:1601.04301v1, pp. 1-12, 2016.
[20] L. G. Zucker, "Production of trust: Institutional sources of economic structure," Organizational Behavior, vol. 8, pp. 1840-1920, 1986.
[21] M. Alhabeeb, A. Almuhaideb, P. Le and B. Srinivasan, "Information Security Threats Classification Pyramid," in 24th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2010.
[22] M. de Bruijne, M. van Eeten, C. Hernández Gañán and W. Pieters, Towards a new cyberthreat actor typology. A hybrid method for the NCSC cyber security assessment, Delft: TU Delft, 2017.
[23] M. Januszewska, I. Michalska-Dudek and R. Przeorek-Smyka, "Online Travel Agent and Travel Metasearch Engine as a Examples ofInformation and Communication Technologies Implementation in the Distribution of Travel Agencies Offers," in Proceedings of the 10th International Conference Liberec Economic Forum , Liberec, 2011.
[24] M. K. O. Lee and E. Turban, "A Trust Model for Consumer Internet Shopping," International Journal of Electronic Commerce, vol. 6, no. 1, 9 2001.
[25] N. Y. Conteh i P. J. Schmick, „Cybersecurity:risks, vulnerabilities and countermeasures to prevent socialengineering attacks," International Journal of Advanced Computer Research, Vol 6(23) , pp. 31-38, 2016.
[26] P. Beynon-Davies, Database Systems (3rd ed.), New York: Palgrave Macmillan, 2003.
[27] P. Kotler and G. Armstrong, Principles of Marketing, Englewood Cliffs: Prentice Hall, 1994.

[28] P. Kotler, „the New marketing and sales-strategies and tactics,” w XIX Seminar of the Series Autorities, 2006.

[29] P. M. Doney and J. P. Cannon, "An examination of the nature of trust in buyer-seller relationships," Journal of Marketing, vol. 61, no. 2, pp. 35-51, 1997.

[30] P. Mateti, „Unix. The world's first computer virus,” w The Unix Haters Handbook, Dayton, Wright State University, 2001.

[31] P. Toršić, “On the Programming Models, Smart Middleware and Self-Healing Capabilities for the Next-Generation Internet-of-Things,” in Computing Conference 2018 10-12 July 2018, London, 2018.

[32] Q. Li and Y. Sun, “An Agent Based Intelligent Meta Search Engine,” in Proceedings of the 2012 international conference on Web Information Systems and Mining, Berlin, 2012.

[33] R. H. Weber, "Internet of Things – New Security and Privacy Challenges," Computer Law & Security Review vol. 26, issue 1, pp. 23-30, 2010.

[34] S. Dayal, H. Landesberg and M. Zeisser, "How to Build Trust Online," Marketing Management, Fall, pp. 64-69, 1999.

[35] S. Gerić and Ž. Hutinski, “Information system security threats classifications,” Journal of Information and Organizational Sciences vol. 31, pp. 51-61, 2007.

[36] S. Shah Alam and N. Mohd Yasin, "What factors influence online brand trust: evidence from online tickets buyers in Malaysia," Journal of theoretical and applied electronic commerce research J. theor. appl. electron. commer. res. vol.5 no.3, pp. 78-89, 2010.

[37] S. Sicari, D. Rizzardi, D. Miorandi, C. Cappicillo and A. Coen-Porisini, “A secure and quality-aware prototypical architecture for the IoT,” Information Systems vol. 58, pp. 43-55, 2016.

[38] W. H. Grudzewski, I. K. Hejduk, A. Sankowska and M. Wańtuchowicz, Zarządzanie zaufaniem w przedsiębiorstwie, Kraków: Oficyna Wolters Kluwer Business, 2009.

[39] Z. K. Zhang, "IoT Security: Ongoing Challenges and Research Opportunities," in IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA 2014), 2014.