CYBERSECURITY OF SMALL AND MEDIUM ENTERPRISES IN THE ERA OF INTERNET OF THINGS

František Kasl*[1]

Abstract: *The issues related to cybersecurity are being amplified by the growing role of the Internet of Things devices in current digital economy. The focus of this contribution is to examine the challenges of IoT environment for the corporate cybersecurity from the legal perspective with regards to the specific role of small and medium enterprises. It provides an introduction into the environment of SMEs and the transformation of their operations through new technologies, followed by highlights of the cybersecurity challenges brought by the IoT. Core part of the contribution is an analysis of the applicable legal frameworks and discussion of the broader picture with regard to this specific perspective on the regulation of corporate cybersecurity.*

Keywords: *cybersecurity, small and medium enterprises, Internet of Things*

I. INTRODUCTION

It is difficult to imagine doing business in the modern EU economy without the involvement of ICT technology and the internet connection. At the same time, the modernisation continues on a relentless pace, bringing to the markets countless new products and solutions. More and more devices contain communication modules that connect them to the internet or similar network. These products are widely referred to as the Internet of Things ("IoT"), a growing mesh of interconnected cyber-physical artefacts that bring the society closer to omnipresent digitalisation.

The growing importance of cybersecurity measures in face of these technological changes draws a lot of attention, particularly from three perspectives; the customers' perspective focused on the issues of privacy, data protection and safety; the producers' perspective focused on the issues of liability and standardization; and the state perspective focused on the national defence and cybercrime suppression. Rather under-researched remains the particular position of the small and medium enterprises ("SMEs"), despite their often unique role with regard to this technological transformation. Many SMEs are positioned in between the above mentioned perspectives, representing small-size corporate customers that have often similar position to the individuals; producers with uncomplicated operations and limited capacities; and subjects to the state cybersecurity strategy that may not be regarded as critical components individually, but which represent crucial assets, if perceived as a group.

* Ing. Mgr. František Kasl, Ph.D. student, Institute of Law and Technology, Faculty of Law, Masaryk University in Brno, Brno, Czech Republic

[1] This contribution follows from a presentation on 18th May 2017 at the TILTing Perspectives 2017 conference in Tilburg, the Netherlands. It is a result of a research project *Zajištění bezpečnosti osobních údajů v podnikových sítích malých a středních podniků v kontextu internetu věcí* [Ensuring the security of personal data in corporate networks of small and medium-sized enterprises in the context of the Internet of Things] funded by Masaryk University in Brno, Czech Republic.

The focus of this contribution is to examine the challenges of IoT environment for the corporate cybersecurity from the legal perspective with regards to the specific role of SMEs, to subsequently identify possible issues that need to be addressed and to discuss their specifics.

This article is structured as follows: Section 2 provides an introduction into the environment of SMEs and the transformation of their operations through new technologies. Section 3 highlights the cybersecurity challenge brought by the IoT. Section 4 analyses the applicable legal frameworks that are relevant to this setting. Section 5 then briefly discusses the broader picture of the SME cybersecurity challenge.

II. SMALL AND MEDIUM ENTERPRISES IN THE DIGITAL AGE

II. 1 Definition of a Small or Medium Enterprise

The SMEs are regarded as statistically and legally important category of enterprises[2] that should be perceived and approached in specific way in order to accommodate for their differences from large enterprises, holdings and other economic entities. These differences reflect primarily the limited resources that these enterprises operate with. The category covers diverse businesses that together build up the core of market economies, accounting for majority of employment, innovation and economic interaction. According to the statistics of European Commission, SMEs in Europe accounted in 2015 for 99.8% of all enterprises, 57.4% of value added, and 66.8 % of employment in the non-financial business sector.[3]

Small and medium-sized enterprises were defined for the purposes of unified interpretation of the European law in the Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises. The indicators of an SME are the "staff headcount criterion"[4] and "financial criterion".[5] There are three subcategories; a medium-sized enterprise employs fewer than 250 persons and has simultaneously an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.[6] A small enterprise then counts fewer than 50 employees and an annual turnover and/or annual balance sheet total with less than EUR 10 million.[7] Finally, enterprises, which employ fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million, are categorized as microenterprises.[8] For the purpose of better contextual percep-

[2] *"An enterprise is considered to be any entity engaged in an economic activity, irrespective of its legal form. This includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity."* Art. 1 of the Annex to the Commission Recommendation 2003/361/EC.

[3] MULLER, P., et al. Annual Report on European SMEs 2015 / 2016. In: *European Union* [online]. 2016 [2017-09-27]. Available at: <https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf>, p. 8.

[4] Recital 4 Commission Recommendation 2003/361/EC.

[5] Ibid.

[6] Art. 2(1) of the Annex to the Commission Recommendation 2003/361/EC.

[7] Art. 2(2) of the Annex to the Commission Recommendation 2003/361/EC.

[8] Art. 2(3) of the Annex to the Commission Recommendation 2003/361/EC.

tion of the subsequent paragraphs, please keep in mind, that according to the above mentioned statistic, around 90 % of all European enterprises in the non–financial sectors are microenterprises with less than 10 employees.[9] Furthermore, large part of the innovative potential of an economy comes from the start-ups that count among these microenterprises.

To talk about SMEs means to talk about countless unique business settings that include the smallest two-person start-ups as well as established medium enterprises with complex corporate structure. Simultaneously, the role of digitalisation in the operations of SMEs is very diverse, reflecting many new emerging business models. In a sense the SMEs play a uniquely dichotomic role in the face of modernization, as the category includes the most progressive and innovative start-ups and pioneers of digital economy, as well as many very static entities, that stick to the traditional business models and are oblivious to or purposely rejecting the new technologies.

The aim of this article is to discuss cyber security issues related to doing business as a SME in the era of IoT. There are apparent limits to the aggregate use of the term SME in this context. The discussed features of ICT technologies are not relevant for all entities that fall under this category. However, a search for more fitting categorization is probably futile, given that the determining characteristics are related to multiple properties of the given enterprise, particularly the dependence of its business operation on ICT, branch and location of operations, or use of connected devices in the business operations. The point is that in the end, situation of every business entity is specific. Nevertheless, given that the category of SMEs is repeatedly used as framework of reference in the legislation, policy papers and academic literature relevant to the topic of this contribution, the term is similarly employed in the following text.

II. 2. Modern Trends, Digital Workplace and the Time of IoT

With full knowledge of these limits of the general SME categorization to any abstraction from micro to macro perspective of the aggregate tendencies among the SMEs, as well as differences between the member states of the EU, there seems to be strong general trend towards modernisation, innovation and digitalisation of the SME operations throughout the EU.[10]

These trends are closely linked to shifts towards greater connectivity, interoperability and inter-dependence as well as adaptability, customization and just-in-time logistics. The role of the ICT in these shifts is pivotal, as they result from the commercialization of the internet network and its relentless development and expansion. The digitalisation of

[9] MULLER, P. et al. *Annual Report on European SMEs 2015 / 2016*. p. 6.

[10] The Commission's Europe's Digital Progress Report 2017 provides a summary snapshot of digitalisation development in EU businesses. See EUROPEAN COMMISSION. Integration of Digital Technology. In: *Europe's Digital Progress Report 2017* [online]. 2017 [2017-12-02]. Available at: <https://ec.europa.eu/digital-single-market/en/news/europes-digital-progress-report-2017>, slides 6 and 7.

the market economy revolves around data processing and transfer.[11] Business operations involve the broadest possible variety of data, ranging from technical metadata, through business confidential or protected data[12] to personal data.[13] These data form the basis of information assets, which are increasingly essential for the functions of an enterprise.

It is becoming strongly apparent that the current state of the digital economy is merely an intermediate stage on a way towards a state of greater omnipresent connectivity and digital data-driven economy. The role of the ICT grows through introduction of numerous new ideas and concepts, ranging from the cloud storage to machine learning or big data analysis. The stream of new inventions and products is overwhelming and highly heterogeneous. One large group that enjoys increasing attention is the loosely defined category of Internet of Things.

II. 3 Internet of Things

The Internet of Things is a popular term for what remains a challenging concept to be satisfyingly defined. Furthermore, a variety of other terms are often used in similar context, particularly "cyber-physical systems"[14], "ubiquitous computing"[15], "ambient intelligence"[16] or "eObjects"[17]. A comprehensive study of the available definitions of IoT by IEEE[18] conveys the diversity that indicates a frequent bias towards specific aspects meant to be emphasized.[19] The IEEE distilled from these two neutral definitions. From a perspective of small environment with low complexity; *"[a]n IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique*

[11] Vice-President of the European Commission Andrus Ansip in his speech at Bruegel annual meeting pointed out that: *"If I had to express my views about the digital future – that of Europe or indeed, of the whole world - I could do it with one word: data. The digital economy revolves around data. It is the driving force behind those three main elements of productivity, innovation and digitalisation."* See ANSIP, Andrus. Speech by Vice-President Ansip at Bruegel annual meeting: "Productivity, innovation and digitalisation - which global policy challenges?" In: *European Commission* [online]. 9.7.2015 [2017-12-02]. Available at: <https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/speech-vice-president-ansip-bruegel-annual-meeting-productivity-innovation-and-digitalisation-which_en>.

[12] E.g. financial data, strategic documents, intellectual property or business know-how.

[13] According to Art. 4(1) GDPR: *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

[14] MINERVA, R., BIRU, A., ROTONDI, D. Towards a definition of the Internet of Things (IoT). In: *IEEE* [online]. 2015 [2017-12-01]. Available at: <http://iot.ieee.org/definition.html>, p. 71.

[15] See WEISER, M. The computer in the 21st century. *Scientific American.* 1991, Vol. 265, No. 3.

[16] INFORMATION SOCIETY. IST Advisory Group Strategic orientations and priorities for IST in FP6. In: *European Commission* [online]. 2002 [2017-12-02]. Available at: <http://cordis.europa.eu/pub/ist/docs/istag_kk4402456encfull.pdf>, p. 9.

[17] MANWARING, K., CLARKE, R. Surfing the Third Wave of Computing: A Framework for Research into eObjects. *Computer Law & Security Review: The International Journal of Technology Law and Practice.* 2015, Vol. 31, No. 5, [2017-12-02]. Available at: <http://www.sciencedirect.com/science/article/pii/S0267364915001144>, p. 598.

[18] Institute of Electrical and Electronics Engineers.

[19] MINERVA, R., BIRU, A., ROTONDI, D. *Towards a definition of the Internet of Things (IoT),* p. 70.

identification and sensing, information about the 'Thing' can be collected and the state of the 'Things' can be changed from anywhere, anytime, by anything."[20] This description is focused on the capacities of a specific device or artefact and its features added through the connectivity. The large environment scenario definition offers a broader picture: *"Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.*"[21] It is particularly this definition that is relevant to the perception of IoT in business environment and with regard to cybersecurity.

IoT covers a broad spectrum of technological solutions adopted in industrial production, logistics, resource management, retail and beyond.[22] It spans sectors and segments from healthcare, energy distribution, or infrastructure to numerous private consumer uses in safety, convenience and entertainment areas.[23] The implementation into production and the consequent transformation of business operations is often labelled as "Industry 4.0".[24]

The boom of this multi-product category is intertwined with the broader trends towards digitalisation of economy,[25] enhancing or supporting broader adoption of other new technologies. Among the existing devices numerous feature cloud storage and computing, machine-to-machine communication, robotic automation, algorithmic machine learning, profiling and big data mining or other particular new technologies.[26]

---

[20] MINERVA, R., BIRU, A., ROTONDI, D. *Towards a definition of the Internet of Things (IoT),* p. 74.

[21] Ibid.

[22] For some specific examples of industrial application see e.g. MERCER, C. Internet of things examples: 14 best uses of IoT in the enterprise. In: *ComputerworldUK* [online]. 27. 6. 2017 [2017-12-09]. Available at: <https://www.computerworlduk.com/galleries/cloud-computing/internet-of-things-best-business-enterprise-offerings-3626973/>, or LIBELIUM. 50 Sensor Applications for a Smarter World. In: *Libelium* [online]. 2017 [2017-12-09]. Available at: <http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/>.

[23] For more detailed overview of the main areas of application see BEECHAM RESEARCH LTD. M2M Sector Map. In: *Beecham Research Shaping the IoT Future* [online]. 2011 [2017-12-02]. Available at: <http://www.beecham-research.com/download.aspx?id=18>.

[24] This term is employed particularly in Germany. See PLATFORM INDUSTRIE 4.0. IT-Security in der Industrie 4.0 Handlungsfelder für Betreiber. In: *Bundesministerium für Wirschaft und Energie* [online]. 2016 [2017-10-01]. Available at: <http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/leitfaden-it-security-i40.pdf?__blob=publicationFile&v=6>.

[25] For current progress in various segments see the aforementioned EUROPEAN COMMISSION. *Integration of Digital Technology.*

[26] Various attributes of IoT summarized e.g. MANWARING, K., CLARKE, R. *Surfing the Third Wave of Computing: A Framework for Research into eObjects,* pp. 599–601. See also MINERVA, R., BIRU, A., ROTONDI, D. *Towards a definition of the Internet of Things (IoT),* p. 41 et seq.

If connectivity is defining aspect of this new technology, then its core revolves around sharing and processing of immense amounts of data relevant to the enterprise, user or situation. The IoT devices not only operate with the available corporate, technical and personal data, but to a large degree create additional data inputs that may directly or indirectly conceal valuable corporate or personal information.[27] Ceaseless connectivity also means intensive and varied interaction with the corporate networks, urging for more flexible network architecture. This in consequence complicates corporate network traffic oversight and brings new challenges to cyber security design.[28]

Enterprises of various sizes come as key players in the IoT era of transformation; they take up the roles of developers, producers, distributors, promoters, as well as customers.[29] The field of industrial IoT is growing rapidly,[30] as the implementations lead to increases in efficiency, productivity, precision or to optimization of costs.[31] The early adoption of large scale IoT corporate solutions will probably be pioneered by the large enterprises. There are, however, many situations, when many the SMEs are likely to soon get in close interaction with IoT devices.

II. 4 IoT in the Corporate Networks of the SMEs

It is difficult to predict the final outcome of the trend towards higher digital connectivity in different sectors of the economy, yet it is reasonable to expect that the unavoidable development of the business environment through market forces will eventually lead to an extensive transformation of the traditional business models. This process is already well underway and it seems unlikely that the majority of SMEs will be able to do business as usual without joining this trend.

The digitalisation of the business environment, as well as gradual introduction of IoT in the last decade, lead to a lot of buzz and activity on the part of European, national as well as commercial institutions and initiatives. Collaboration associations, support programs, innovation workshops, financing projects, conferences and numerous other activities surround this trend and navigate its course. There are many new business ventures, start-up projects and research initiatives that fuel the process through implementation of IoT components in their business operations or their products and propagation.[32] The in-

[27] E.g. MARAS, M. Tomorrow's Privacy. Internet of Things: security and privacy implications. *International Data Privacy Law.* 2015, Vol. 5, No. 2, p. 100.

[28] E.g. PLATFORM INDUSTRIE 4.0. *IT-Security in der Industrie 4.0 Handlungsfelder für Betreiber,* p. 6–7.

[29] WORLD ECONOMIC FORUM. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. In: *World Economic Forum* [online]. 2015 [2017-12-10]. Available at: <http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf>, p. 14 et seq.

[30] COLUMBUS, L. Roundup Of Internet Of Things Forecasts And Market Estimates, 2016. In: *Forbes* [online]. 2016. [2017-12-09]. Available at: <https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#7f4b526c292d>.

[31] WORLD ECONOMIC FORUM. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services,* p. 3.

[32] E.g. the European Commission created a dedicated Focus Area on IoT a part of its Work Programme 2016-17 under Horizon 2020 aimed at large-scale IoT pilot projects in various areas. See EUROPEAN COMMISSION. Horizon 2020 Work Programme 2016-2017: Internet Of Things Large Scale Pilots. In: *Digital Single Market* [online]. 2015 [2017-12-02]. Available at: <https://ec.europa.eu/digital-single-market/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots>.

novative SMEs are seen as a crucial component of the development of Digital single market and the European Union provides various funding instrument for these entities.[33] These pioneer SMEs are at the forefront of the transformation and they need to actively surpass the dangers of new forms of digital connectivity. However, even if a SME does not directly invest into an introduction of the IoT devices to its business operations, there are numerous indirect ways that may make this trend relevant for that given enterprise. Aside from the adoption of new systems and frameworks by the suppliers, customers and other business partners of the enterprise, the actions and requirements of the employees are likely to eventually bring the IoT devices into relevance for many corporate networks of any size.

The corporate BYOD (Bring-Your-Own-Device) policies are already considerably spread and with the increasing dependence of individuals on their personalized devices, the demand towards open BYOD policies by employees are likely only to increase.[34] Given the boost it offers to productivity and employee loyalty,[35] this type of policy is here to stay and specific security issues related to its implementation need to be considered.[36] It is particularly the SME business environment, where the BYOD approach could stay prevalent. This assumption is based on two arguments. Firstly, the SMEs, particularly the smallest, tend to have difficulties with clearly setting apart the private and corporate data handled by the employees or owners.[37] Secondly, the open BYOD policies allow for taking advantage of new technologies without additional investment into the corporate equipment. This form of expense savings can be relevant in enterprises with very limited budget, also particularly the microenterprises.

The assumption therefore goes that the corporate networks of many SMEs are in not so distant future likely to integrate or interact with multiplicity of IoT devices. One of the eventual impacts of this transformation will be the further increasing importance of data management and data security for the business operations of the enterprise.

---

[33] For more see e.g. EUROPEAN COMMISSION. Accelerating innovation in Europe: Horizon 2020 SME Instrument impact report. In: *European Commission* [online]. 2017 [2017-12-09]. Available at: <https://ec.europa.eu/easme/sites/easme-site/files/accelerating_innovation_in_europe_horizon_2020_smei_impact_report.pdf>.

[34] ZAHADAT, N. et al. BYOD security engineering: A framework and its analysis. *Computers & Security*. 2015, Vol. 55, [2017-12-09]. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404815000978>.

[35] Based on the data gathered in a questionnaire among employees by the Economist 45% of them did believe that mobility makes them more productive and 30% would not work for a company, which does not allow BYOD. See ECONOMIST INTELLIGENCE UNIT. Mobility, performance and engagement. In: *The Economist* [online]. 27. 4. 2016 [2017-12-09]. Available at: <https://www.eiuperspectives.economist.com/technology-innovation/mobility-performance-and-engagement/white-paper/mobility-performance-and-engagement>.

[36] For detailed analysis of security issues related to BYOD policy see ZAHADAT, N. et al. *BYOD security engineering: A framework and its analysis*.

[37] CLARKE, R. The prospects of easier security for small organisations and consumers. *Computer Law & Security Review*. 2015, Vol. 31, No. 4, [2017-12-09]. Available at: <http://www.sciencedirect.com/science/article/pii/S0267364915000849>, p. 539; or SANGANI, N. K., VIJAYAKUMAR, B. Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informatica Economica*. 2012, Vol. 16, No. 2, p. 59.

III. THE DARK SIDE OF THE CONNECTIVITY

The dependence of the economy on connectivity and data processing has also its dark side. News about security vulnerabilities being exposed and large datasets being breached became unfortunately something of everyday news.[38] Available data from the first half of 2017 signal further massive increase in the number of detected data breaches[39] and particularly in the amount of records stolen or lost.[40] If Weber noted that year 2014 and 2015 were referred to as Year of the Breach and Year of the Breach 2.0.,[41] then the trend sadly goes on and it goes strong. The picture painted by available reports is, however, likely to be still significantly understating the size of the real problem. There are clearly more events going unreported,[42] particularly small size incidents typical for SMEs.

The "price tag" put on cybercrime by McAfee in 2014 was around $400 billion in annual costs.[43] Even if these estimates were described as greatly approximate and based on incomplete information about intangible assets,[44] they paint a picture of a massive burden. Also, many incidents leading to loss or disclosure of data are not due to external attack, but often a consequence of accidental data manipulation by insiders or other inadequate data management settings,[45] and do not thereby count as cybercrime. These internal threats are often understated,[46] which further manifests the gravity of the need for adequate cyber security management in many entities.

III. 1 Cybersecurity

The area of expertise dealing with these threats is commonly termed cybersecurity. Because of the complexity of the issue, variability of settings and fast pace of change, it takes many forms. Currently no generally accepted definition of this discipline ex-

[38] A sobering detailed statistics about data breaches assorted by year, industry, location or size are available at GEMALTO. Data Breach Statistics by Year, Industry, More. In: *Breach Level Index* [online]. 2017 [2017-12-09]. Available at: <http://breachlevelindex.com>.

[39] Gemalto identified 918 data breaches worldwide, compared with 815 in the last six months of 2016. See GEMALTO. 2017 Poor Internal Security Practices Take a Toll. In: *Breach Level Index* [online]. 2017 [2017-09-17]. Available at: <http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf>, p. 3.

[40] The same report states that some 1.9 billion data records were lost or stolen during the first half of 2017, compared with mere 721 million during the previous six months, giving an increase of 164%. See GEMALTO. *2017 Poor Internal Security Practices Take a Toll.*

[41] WEBER, R. H. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*. 2016, Vol. 2016, No. 32, p. 715.

[42] The following study gives thorough insight into the size of the possible unreported part of data breaches. See BISOGNI, F., ASGHARI, H., VAN EETEN, M. J.G. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*: *WEIS 2017*. San Diego: University of California.

[43] MCAFEE. Net Losses: Estimating the Global Cost of Cybercrime. In: *McAfee* [online]. 2014 [2017-12-09]. Available at: <https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf>, p. 2.

[44] For more thorough description of the limits of any such valuation see BREWSTER, Tom. Is the global cost of cybercrime really £266bn a year? No, it isn't. In: *The Guardian* [online]. 2014 [2017-12-09]. Available at: <http://www.theguardian.com/technology/2014/jun/09/global-cost-of-cybercrime-266bn>.

[45] GEMALTO. *2017 Poor Internal Security Practices Take a Toll*, p. 4.

[46] For a detailed guide through many traditional cybersecurity misconceptions see CRUME, J. *Inside Internet Security: What Hackers Don't Want You To Know*. Addison-Wesley Professional, 2000.

ists.[47] Herr and Friedman openly claim that *"[c]ybersecurity is an often abused and much misused term that was once intended to describe and now serves better to confuse."*[48]

Anderson on his blog recently stated: *"My talk started off from Ame Elliott's argument yesterday that "cybersecurity" is an unhelpful and indeed militaristic reframing of what we do. This resonates with the last 25 years of my life through the crypto wars, the birth of security economics and my book on security engineering."*[49] Anderson prefers to use the term security engineering, a cross-disciplinary endeavour towards building resilient and dependable ICT systems, to describe the actions needed to protect from malicious or accidental cybernetic incidents.[50]

If we accept the limitation of the term cybersecurity and the problematic connotation it may have in some settings, a working definition for the purpose of this paper can be borrowed from ITU: *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."*[51] The term "assets" in this context includes hardware, software, networks, data, personnel or other parts of the entity's internal networks and operations.[52] The aim of cybersecurity is to protect functions and functioning of the system. This is also commonly described by the "CIA triad" of security objectives; (i) confidentiality, (ii) integrity and (iii) availability.[53]

III. 2 Cybersecurity Threats to Corporate Networks

The spectrum of potential vulnerability vectors that may affect the business through its corporate network is broad and continuously increasing. For the purpose of a general overview, an illustrative system of three threat targets was adopted for this article.[54] These categories do not encompass fully all potential threats and may also overlay in some cases; however, they allow better perception of the specific roles of the SMEs in the overall cybersecurity landscape.

---

[47] SILVA, K. Europe's fragmented approach towards cybersecurity. *Internet Policy Review*. 2015, Vol. 2, No. 4, [2017-12-09]. Available at: <http://policyreview.info/articles/analysis/europes-fragmented-approach-towards-cybersecurity>.

[48] HERR, T., FRIEDMAN, A. Redefining Cybersecurity: The American Foreign Policy Council Defense Technology Program Brief. In: *American Foreign Policy Council* [online]. [2017-12-09]. Available at: <http://www.afpc.org/publication_listings/viewPolicyPaper/266413>.

[49] ANDERSON, R. Security and Human Behaviour 2017. In: *Light Blue Touchpaper: Security Reseach, Computer Laboratory, University of Cambridge* [online]. 25. 5. 2017 [2017-12-09]. Available at: <https://www.lightbluetouchpaper.org/2017/05/25/security-and-human-behaviour-2017/>.

[50] ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd edition Indianapolis: Wiley Publishing, 2008. p. 3.

[51] INTERNATIONAL TELECOMMUNICATION UNION. Definition of cybersecurity. In: *ITU* [online] [2017-12-06]. Available at: <http://www.itu.int:80/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>.

[52] Ibid.

[53] Ibid.

[54] The systematics is based on the threat target identifier adopted by the unit of Cyber Security Assessment Netherlands. See VAN DER MEULEN, N., A JO, E., SOESANTO, S. Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. In: *Committee on Civil Liberties, Justice and Home Affairs, European Parliament* [online]. 2015 [2017-12-09]. Available at: <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf>, p. 30.

First category can be described as the threats affecting primarily the customers or individuals of the targeted entity. These interventions include all forms of data breach, product malfunction or service downtime.[55] SMEs have access to and process various volumes and scopes of personal data. The operations may be limited to data of few individuals, particularly the owners or employees, and the potential threat of unauthorized access to these data may present a limited risk to the affected individuals. Occasionally, however, a company may operate with large databanks about countless individuals or process highly sensitive data.[56] The SME may also have authorization and access to databases or networks managed by larger entities and their network may therefore serve as an access point to otherwise well protected systems.[57]

The second type of threats covers those being aimed at the corporations as producers or economic entities. The spectrum of manifestations encompasses the corporate espionage,[58] theft of intellectual property,[59] malicious interruption of business operations,[60] ransomware[61] and other malware aimed at financial gain, or various forms of social engineering attacks.[62] Similarly as with access to personal data databases, the authorizations and access of SME in the role of suppliers makes them potential gateway into the corpo-

[55] A data breach primarily affects the privacy and virtual identity of the data subject, putting them at risk of unauthorized profiling or identity theft. Similarly, a malfunction presents a threat of injury or damage to property of the user. Service downtime can be largely problematic e.g. by logistics, administration tools, medical equipment or other dependable analytic systems.

[56] Various professionals or small enterprises operate with highly sensitive data, e.g. lawyers, doctors, accountants, testing or research labs.

[57] Popular example is the hack of Target through HVAC Company. See KREBS, B. Target Hackers Broke in Via HVAC Company — Krebs on Security. In: *Krebs on Security* [online]. 2. 5. 2014 [2017-12-09]. Available at: <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company>.

[58] See e.g. DEPARTMENT OF JUSTICE, U.S. ATTORNEY'S OFFICE. Manhattan U.S. Attorney Announces Arrest Of Macau Resident And Unsealing Of Charges Against Three Individuals For Insider Trading Based On Information Hacked From Prominent U.S. Law Firms. In: *Southern District of New York* [online]. 27. 12. 2016 [2017-12-09]. Available at: <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against>.

[59] GRIFFIN, A. HBO hack behind Game of Thrones season 7 script leak is a sign of things to come, warn cyber security experts. In: *The Independent* [online]. 2017 [2017-12-09]. Available at: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/hbo-hack-game-thrones-season-7-script-leak-cyber-security-experts-got-spoilers-media-tv-series-a7871086.html>.

[60] A prime example is the recent massive "wiper" attack dubbed NotPetya. This malware encrypted data, but did not allow a way to recover them. See TECHNOLOGY. Cyber-attack "about data not money". In: *BBC News* [online]. 2017 [2017-12-09]. Available at: <http://www.bbc.com/news/technology-40442578>.

[61] Ransomware stands for malware that encrypts valuable data and requires ransom for the decryption key. This type of malicious activity became recently massively widespread. Media attention was grabbed particularly by the WannaCry ransomware peaking in May 2017. See TECHNOLOGY. Massive cyber-attack hits 99 countries. In: *BBC News* [online]. 2017 [2017-12-09]. Available at: <http://www.bbc.com/news/technology-39901382>.

[62] Social engineering is particularly effective form of illicit cyber activity. It relies on the manipulation of the personnel into disclosure of sensitive information or opening the network to vulnerability. It takes many forms that range from simple phishing email to complex tailor-made scam scenarios. See e.g. HADNAGY, C. *Social engineering The Art of Human Hacking*. Indianapolis: Wiley Publishing, 2011; or MOUTON, F., LEENEN, L., VENTER, H. S. Social engineering attack examples, templates and scenarios. *Computers & Security*. 2016, Vol. 59, [2017-12-09]. Available at: <https://www.sciencedirect.com/science/article/pii/S0167404816300268>.

rate networks of large enterprises.[63] At the same time, the SMEs themselves do possess assets that make them interesting targets for malicious attacks. The SMEs may be less threatened by targeted tailor-made hacking, but nonetheless face a growing avalanche of mass distributed malware and spam, particularly ransomware or social engineering attacks.

The last category encompasses threats that are relevant from the national security perspective.[64] This is mainly the case, if the network devices become enslaved in malicious botnet,[65] which can then accumulate the joined capacity of the swarm of devices for various nefarious purposes.[66] These include, but are not limited to DDoS attacks on high profile targets or critical infrastructure, distribution of malware or spam, or storage space for illegal content.[67] If numerous SMEs become likely target for botnet building malware, the aggregate capacity of this network is likely to become subject of interest for the national cybersecurity units.[68]

Malware that does not manifest its presence to the user (like e.g. ransomware does) is more likely to stay undisturbed and effective and multiple devices in corporate network of the SME make one successful infection easily distributable throughout the local network, increasing the effectivity of the attack. The SMEs represent a large category of economic entities with limited capacity for cybersecurity investment and generally lower awareness to cybersecurity threats. Data breach detection is difficult even in large entities and the usual time to identify such an incident is measured in months after its occurrence.[69] If we consider, that detection of any stealthy incident is unlikely without advanced cybersecurity tools, which the SME usually do not possess, there are possibly many SME networks infected by various forms of malware or botnet command without knowledge.

---

[63] The supply chain cybersecurity plays an increasing role in the interconnected and interdependent economy. Numerous cyber incidents by large entities originate through weak protection in their supply chain, often by SMEs. For more see e.g. PURDY, A. The Global Cyber Security Challenge: It is time for real progress in addressing supply chain risks. In: *Huawei Technologies* [online]. 2016 [2017-12-09]. Available at <http://www-file.huawei.com/~/media/CORPORATE/PDF/cyber-security/the-global-cyber-security-challenge-en.pdf?la=en>; SHACKLEFORD, D. Combatting Cyber Risks in the Supply Chain. In: *SANS Institute* [online]. [2017-12-09]. Available at: <https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252>.

[64] Such threats endanger the availability, integrity or confidentiality of essential services, critical infrastructure, national security facilities, public safety, order or legal and democratic functions of the government. Most states formulate their national cyber security strategy, international cooperation is, however, simultaneously pursued, particularly within NATO. See NATO. Cyber defence. In: *NATO* [online]. 8. 7. 2017 [2017-12-09]. Available at: <http://www.nato.int/cps/en/natohq/topics_78170.htm>.

[65] Botnet stands for robot network, meaning a network of devices that become controlled from a remote command & control server, usually without direct knowledge of the owner and user of such a device.

[66] Prime example is the 2016 massive DDoS attack using the Mirai botnet of IoT devices. See WOOLF, N. DDoS attack that disrupted internet was largest of its kind in history, experts say. In: *The Guardian* [online]. 2016 [2017-12-09]. Available at: <http://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.

[67] CENTRO NAZIONALE ANTIBOTNET. What botnets are. In: *Centro Nationale Antibotnet* [online]. [2017-12-09]. Available at: <http://www.antibot.it/en/content/what-botnets-are>.

[68] This was the case in aforementioned Mirai botnet. See eg BRACY, J. Why securing IoT is a national-security imperative. In: *The International Association of Privacy Professionals* [online]. 24. 10. 2016 [2017-12-09]. Available at: <https://iapp.org/news/a/why-securing-iot-is-a-national-security-imperative/>.

[69] A mean time to identify a data breach was by Ponemon at 201 days in 2016. See PONEMON INSTITUTE. 2016 Cost of Data Breach Study: Global Analysis. In: *IBM* [online]. 6. 2016 [2017-12-09]. Available at: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=sel03094wwen>, p. 23.

III. 3 SMEs as Victims of Cybercrime

There are currently large limits to statistical assessment of corporate cybercrime or cybersecurity in any given area, particularly with regard to SMEs. Nonetheless, as already indicated in beginning of this section, the current trends in cybercrime are overwhelmingly towards continuous increase in its frequency, sophistication, impact as well as scope. In this regard, many of the SMEs present intersection of parameters that make them into highly likely target of cybercrime. It is because they on one hand operate similarly as the large entities with databases of valuable data, but also because breach of their network may provide authorization or access throughout the supply chain to corporate networks of more valuable targets. Furthermore, they are also usually more likely to possess adequate financial assets to be stolen or extorted as ransom than individual users. In general, the fact that SME networks are corporate networks, which usually comprise of multiple devices and may offer access to larger volumes of data and more valuable assets than in case of an individual, makes these networks into valuable targets for cybercrime.

On the other hand, the SME usually suffer from disadvantages that are close to the individual users. It is neither surprising nor revealing that the SME dispose of limited resources and insufficient awareness of cybersecurity.[70] Beside the limited awareness or budget, additional cause may lay in low priority of cybersecurity in comparison to other regulatory burdens and compliance obligations that are more directly linked to doing business as such. Particularly micro enterprises have tendency to practice the approach of "security by obscurity",[71] assuming that their assets are sufficiently insignificant to be a target or simply playing the expected odds of being one of many.

The SME corporate network can suffer from various flaws. It may depend on outdated or ineffective monitoring or cybersecurity tools. It may be subject to lenient BYOD policy that allows compromised devices to be connected without proper control.[72] There may lack education or organisation of the employees, who remain unaware of the threats and uninformed about the proper behaviour to mitigate the risks.[73] All this greatly increases the probability of undetected vulnerability, limits the capacity for timely fix and increases the potential damage. The SMEs are at the same time often highly dependent on the networked devices or software services they use in their business operations, thereby increased risk of malfunction or unavailability of these components increases the risk of business interruption, which may pose existential threat to the SME.

---

[70] Clarke puts it as follows: *"Many other organisations, however, despite having considerable dependence on information and IT, have at best a hazy understanding of IT security."* See CLARKE, Roger. *The prospects of easier security for small organisations and consumers*. p. 538.

[71] Strategy based on the assumed low priority or probability of becoming a target of a malicious attack.

[72] WHITWELL, J. Small businesses should invest in cyber security. In: *The Telegraph* [online]. 2017 [2017-12-09]. Available at: <http://www.telegraph.co.uk/business/open-economy/small-businesses-should-invest-in-cyber-security/>.

[73] This applies particularly to password and communication management and emergency procedure in case of security breach or social engineering scam. See e.g. NIXON, S. Are you an easy hacking target? Cybersecurity tips for small business. In: *The Guardian* [online]. 2017 [2017-12-09]. Available at: <http://www.theguardian.com/small-business-network/2017/sep/08/are-you-an-easy-hacking-target-cyber-security-tips-for-small-business>.

Recent cybersecurity breach survey from the UK[74] provides data to further support above mentioned claims or assumptions. Median annual expenses on cybersecurity by small and micro enterprises were found to be only GBP 200.[75] More tellingly, 39% of small and micro enterprises had no governance or risk management measures implemented, as they considered themselves too small or insignificant.[76] 45% of the small and micro businesses reported data breach in last 12 months.[77] The study identified higher incidence rate among entities that were taking active action towards their cybersecurity, possibly indicating, that those without adequate measures might have simply not identified the fact that their networks were breached.[78]

This very simplified insight into the broad spectrum of traditional attack vectors and their effect on SMEs should underlay two assertions. Firstly, that the SME corporate network is a valuable and frequent target for malicious activities, as it provides access to the data within this network, capacity of the devices in this network that may be used for attacks on third party as well as potential gateway to more valuable, but better protected assets. Conclusion to be drawn from this assertion is that the importance of SME cybersecurity should not be underestimated. The second assertion is that majority of modern cybersecurity threats fall under the 'simple large-scale high-frequency automated attacks' rather than 'complex targeted interventions with specific goal in mind'. The preference of scale operations and exploiting of known vulnerabilities, or deceit of a human, rather than sophisticated hacking, is sufficiently documented.[79] Large portion of the cyberattacks is distributed through mass use of time-proven simple tools and tactics,[80] among which count various forms of malware or ransomware delivered through social engineering tricks as well as botnet DDoS attacks. This, however, means that most targets of cyberattacks are not being selected, but simply caught in widely cast net, therefore "security by obscurity" approach cannot work and high number of SMEs simply means high number of vulnerable targets. Mass incorporation of IoT devices into weakly secured SME corporate networks could therefore prove to be the looming cybersecurity "perfect storm".[81]

---

[74] KLAHR, R. et al. Cyber Security Breaches Survey 2017. In: *UK Department for Culture, Media & Sport* [online]. 2017 [2017-12-09]. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf>.

[75] The value was certainly affected by a fact that 34% of the 829 surveyed micro enterprises reported GBP 0 expenses on cyber security. Also for this fact is the mean value more illustrative than the median, which is GBP 2,600. See KLAHR, R. et al. *Cyber Security Breaches Survey 2017,* p. 21.

[76] This is clearly supporting the assumption of widespread "security by obscurity" approach. See KLAHR, R. et al. *Cyber Security Breaches Survey 2017,* p. 32.

[77] The survey further expressly states that: *"This highlights that there are firms who may mistakenly think that cyber security is not relevant to them, but are also susceptible to breaches."* See KLAHR, R. et al. *Cyber Security Breaches Survey 2017,* p. 39.

[78] KLAHR, R. et al. *Cyber Security Breaches Survey 2017,* p. 40.

[79] EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. The Hague: European Police Office, 2016, p. 8.

[80] SYMANTEC. Internet Security Threat Report 2017 Volume 22. In: *Symantec* [online]. 2017 [2017-12-09]. Available at: <https://www.websecurity.symantec.com/reports-leadgen/istr>, p. 7.

[81] In a way, the cybersecurity of IoT can be perceived as "perfect storm" in itself, even without taking into consideration the particular situation of SMEs. See WEBER, R. H. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*. 2016, Vol. 2016, No. 32, p. 16.

III. 4 IoT Devices as Potential 'Threat Enhancers'

There are substantial concerns that the mass adoption of the IoT devices will lead to additional spike of cybercrime incidents.[82] IoT devices are perceived as 'threat enhancer',[83] as they increase the complexity of the network interaction, diversify the attack vectors and represent computing power that may be easy to enthral.

These devices, linked to the victim networks, may scale up the damage and harm in three major ways. Firstly, if the hacker assumes control over large numbers of vulnerable devices, their computing power can largely enhance the DDoS attacks or other illicit activities.[84] Such 'weaponized IoT devices' may cause massive potential damage to third party victims,[85] whereas this risk only increases with higher penetration of IoT devices in social and economic infrastructures. Secondly, these devices increase the attack surface of the network and their variety creates in combination new vulnerabilities. The third risk comes from the data that these devices collect and process.[86] The omnipresence of IoT sensors and increased documentation of all aspects of activities in digital as well as physical realm through these devices brings new possibilities and features, but also new threats for privacy, secrecy and intimacy on the human as well as business level. This in turn makes these data more valuable and their management and protection more crucial.

So far the cyber criminals, despite several serious incidents,[87] did not yet fully capitalize on the potential of the broad adoption of the IoT devices.[88] There are, however, numerous documented vulnerabilities and security design flaw that highlight frequent absence of adequate security features in IoT devices.[89] The security threat is after all highlighted as the major obstacle to adoption of these devices into corporate networks by the representatives of SMEs themselves.[90]

---

[82] SYMANTEC. *Internet Security Threat Report 2017 Volume 22,* p. 63 et seq; ARBOR NETWORKS. Worldwide Infrastructure Security Report. In: *NETSCOUT* [online]. 2016 [2017-12-09]. Available at: <https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf>, p. 55; or MARINOS, L., BELMONTE, A., REKLEITIS, E. ENISA Threat Landscape 2015. In: *Enisa* [online]. 2015 [2017-12-09]. Available at: <https://www.enisa.europa.eu/publications/etl2015>, p. 74 et seq.

[83] According to the Europol report is the IoT no longer perceived by the law enforcement as an emerging threat, but rather as a regular feature in cybercrime investigations. See EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016,* p. 52.

[84] EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016,* p. 38.

[85] SUTHERHAND, L. The Threat From Weaponized IoT Devices: It's Bigger Than You Think! In: *Security Intelligence* [online]. 20. 7. 2016 [2017-12-09]. Available at: <https://securityintelligence.com/the-threat-from-weaponized-iot-devices-its-bigger-than-you-think/>.

[86] The IoT devices can potentially increase the likelihood or severity of data breaches. See MARAS, M. Tomorrow's Privacy. Internet of Things: security and privacy implications. *International Data Privacy Law*. 2015, Vol. 5, No. 2, p. 101.

[87] E.g. the above mentioned Mirai botnet. See SYMANTEC. *Internet Security Threat Report 2017 Volume 22*, pp. 65–67.

[88] The Europol is warning about inevitability of novel hybrid threats aimed at IoT infrastructures. EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016,* p. 54.

[89] E.g. SCHNEIER, B. The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters. In: *Schneier on Security* [online]. 25. 7. 2016 [2017-12-09]. Available at: <https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html>.

[90] E.g. TREND CONSULTING. Are Europe's SMEs making the most of the Digital Workplace? In: *Aruba* [online]. 2016 [2017-12-09]. Available at: <https://dutchitchannel.nl/563254/rapport-are-europes-smes-making-the-most-of-the-digital-workplace.pdf>, p. 7.

None of the observations about the shortcoming of SME cybersecurity and their vulnerability as cybercrime victims are very new. These issues are discussed since the early era of commercial internet. It is, however, the combination of these attributes of SMEs with the trends towards digital economy, IoT environment and consequential security risks that may result in strongly negative effects against doing business as SME. With regard to the crucial role of SMEs as a whole in the structure of market economy and them being the essential agents of innovation, this matter transcends the challenges faced by individual enterprise and becomes significant from the perspective of cyber security and macroeconomic policies.

IV. RELEVANT LEGAL FRAMEWORKS

The matter discussed in this contribution is subject to group of legal frameworks dealing with various aspects that touch upon the obligations of SMEs for secure processing of data and cybersecurity of their corporate networks. To better illustrate the structure of obligations, once again the illustrative system of three perspectives is adopted.

IV. 1 Customers' Perspective – Personal Data Protection and Safety Regulation

Cybersecurity represents in a way a prerequisite for protection of personal privacy or personal data. Despite difficult interactions between these frameworks secure devices, networks and processing are essential for securing privacy or personal data protection. For this reason, security requirements are an inherent part of the privacy and data protection frameworks.[91]

The EU Data protection reform[92] currently in process[93] is nowadays the most discussed legislative development affecting the SME cybersecurity. It introduces largely uniform tool for encouragement of 'level playing field' on data processing within the EU.[94] The adoption of the General Data Protection Regulation (GDPR)[95], E-Privacy Regulation[96] as well as other related European[97] and national legislation is aimed at providing high level of protection

[91] KUNER, C. et al. Editorial: The rise of cybersecurity and its impact on data protection. *International Data Privacy Law*. 2017, Vol. 7, No. 2, p. 73.

[92] EUROPEAN COMMISSION. Reform of EU data protection rules. In: *JUSTICE Building European Area of Justice* [online]. [2017-12-09]. Available at: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>.

[93] The legislation is due to take effect on 25th May 2018.

[94] EUROPEAN COMMISSION. How will the EU's data protection reform strengthen the internal market? In: *European Commission* [online]. [2017-12-09]. Available at: <http://ec.europa.eu/justice/data-protection/files/4_strenghten_2016_en.pdf>.

[95] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[96] Currently in a form of Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

[97] Particularly the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

to the individual's personal data, their use, processing, distribution and storage. It therefore sets adequate requirements on the corporate level technical and organisational data security measures. The obligations are not a new concept,[98] but the SMEs remain challenged with lack of guidelines for specific interpretation of their obligations.[99]

With regard to cybersecurity, GDPR is aimed towards a specific objective, the security of processing of the personal data of the data subjects and protection of their related rights and freedoms.[100] The obligations that arise to the enterprise in its role as data controller or processor include requirements of adequate technical and organisation measures for securing the personal data processing.[101] Given that personal data processing is in many cases crucial aspect of the core business operations of the entity, this requirement is likely to affect the overall security of the entity's corporate network. The norm follows the risk-based approach, linking the level of required measures appropriate to the risk to the rights and freedoms of the affected data subject.[102] Adoption of suitable risk assessment method is therefore an important step towards compliance, albeit identification of such method is increasingly challenging in face of the transformation brought by the era of IoT.[103] The assessment the data controller or processor has to undertake is multipolar,[104] taking further into consideration the nature, scope, context and purposes of processing as well as available technological solutions and costs related to the implementation of the selected measures.[105] It therefore needs to be mindful of the potential impact of data breach and design its processing operations accordingly in order to adequately prevent unauthorized or accidental destruction, loss, alteration or disclosure or effectively mitigate consequence of such situation, e.g. through encryption, pseudonymisation or backup.[106] Similar requirements are also manifested through the accents on continuous protection, data minimisation and managed limited data accessibility expressed in GDPR as data protection by design and by default.[107]

The required actions are not only technical, i.e. control management, authorization, monitoring or reporting tools, but also organizational. Particularly in prevention of acci-

[98] Currently applicable requirements have been set by Article 17 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[99] ENISA. *Guidelines for SMEs on the security of personal data processing*. 2016, p. 5–6.

[100] Art. 1(1,2) and Art. 5(1)(f) GDPR.

[101] Art. 24 and 32 GDPR.

[102] Art. 32(1) GDPR.

[103] Guidance may be provided by ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches. In: *Enisa* [online]. 2013 [2018-02-27]. Available at: <https://www.enisa.europa.eu/publications/dbn-severity> or other frameworks, models and guidelines. For examples see ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. In: *European Commission* [online]. 2017 [2018-02-27]. Available at: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137>, p. 20.

[104] PAAL, B. P. et al. *Datenschutz-Grundverordnung: DS-GVO*. München: C.H.Beck, 2017. Beck'sche Kompakt-Kommentare. online version. [2017-10-10]. Available in: Beck. Art. 32(B.)(I.) Rn. 26.

[105] Art. 32(1) GDPR.

[106] Art. 32(1)(a-d) GDPR.

[107] Art. 25 GDPR.

dental cyber incidents or protection against social engineering[108] is the aspect of employee management, education, motivation and communication essential.

The compliance regime under GDPR is primarily build on the principle of accountability,[109] requiring the data controller or processor to demonstrate the implemented measures and their adequacy in relation to the processing operations. The regulation was conceived with more lenient requirements towards SMEs in mind.[110] Despite the derogation in record-keeping obligations for SMEs,[111] the SMEs are advised to keep proper records of their organizational and technical measures for ensuring the security of personal data processing and its regular revision.[112] SMEs are also not except from the obligation to implement these measures[113] or from the newly introduced mandatory data breach notification duties.[114]

The SMEs are in somewhat disadvantaged position to larger entities in their quest to properly comply with the GDPR requirements, given their limited budgetary, know-how and particularly personnel assets. For this reason, official guidelines and state sponsored programs with focus on SMEs are crucial for achieving the purpose of the regulation among this large segment of diverse enterprises. ENISA released a study providing general guidance for SMEs to their GDPR related security obligations in December 2016.[115] This document is a needed basic framework for clarification of often ambiguous terms in the GDPR. It does, however, deal only with the general principles and methods of securing the personal data processing. The cybersecurity challenges faced by the SMEs are diverse and more sector and jurisdiction specific guidelines need to follow, to be able to properly communicate the GDPR framework to the SME recipients.

The ENISA guidelines touch upon the issue of IoT devices by identifying the capacity of this technology to further interlink personal data security and underlying corporate network security.[116] The obligations set forward by the data protection framework cannot be perceived in a vacuum, but need to be systematically connected to other requirements on overall corporate network security. The Data protection reform should not end up being perceived by the SMEs as additional administrative burden limiting their capacity to do business, but as an incentive for broadly needed investment into integrated and effective cybersecurity measures that cover vulnerable and valuable assets of the company.

---

[108] MOUTON, F., LEENEN, L., VENTER, H. S. *Social engineering attack examples, templates and scenarios*. p. 207.

[109] Art. 24(1) GDPR.

[110] DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. EU Data Protection Reform: What benefits for businesses in Europe? Fact sheet. In: *European Commission* [online]. 2016 [2017-12-09]. Available at: <http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf>, pp. 5–6.

[111] Art. 30(5) GDPR.

[112] VAN CANNEYT, T., PROVOOST, S. M. Belgian DPA publishes recommendation on GDPR record keeping obligation. In: *Fieldfisher* [online]. 7. 4. 2017 [2017-11-11]. Available at: <http://privacylawblog.fieldfisher.com/2017/belgian-dpa-publishes-recommendation-on-gdpr-record-keeping-obligation/>.

[113] ENISA. *Guidelines for SMEs on the security of personal data processing*. p. 6.

[114] Art. 33 and 34 GDPR.

[115] ENISA. *Guidelines for SMEs on the security of personal data processing.*

[116] ENISA. *Guidelines for SMEs on the security of personal data processing.* pp. 7–8.

However, only by highlighting the urgency of the need for transformation of the use of ICT technology and the benefits for every participating entity and its business model in face of the expansion of IoT can a timely progress on this front be achieved.

Additional to the protection of individual's personal data and privacy does the legal framework include an established mechanism of legal instruments for her or his safety.[117] The rules for product liability apply in case of injury or damage caused by product malfunction. This regime becomes increasingly relevant due to the rise of IoT devices as cyber-physical artefacts. Given that the liability for service or intangible goods like software does not reach the protection in case of tangible products, there is a growing debate concerning the liability distribution in case of defective IoT device.[118]

IV. 2 Producers' Perspective – Sector Specific Regulations

Next to the legal obligations described in the previous section, the enterprises are often subject to sector-specific regulations.[119] Most of the requirements for security of corporate operations in these regulations are formulated as general performance and risk based rules. Overall the corporate cybersecurity in various sectors is generally governed on the self-regulation basis, with each sector or industry adopting guidelines and best practices for appropriate measures, usually with cybersecurity as secondary or implied component.

The SMEs are often further bound on the contractual basis through its subcontracting relationship to larger enterprise, particularly in case of ICT maintenance or administration services.[120] The compliance with these requirements is usually manifested through adherence to recognized standards and technical norms, in case of technical and organisational cybersecurity measures particularly to the ISO/IEC 2700x family or ISA/IEC 62443.[121]

---

[117] Product liability directive 85/374/EES, as well as several sector specific frameworks, e.g. directive 2007/46/EC for motor vehicles or 2007/47/EC concerning medical devices.

[118] This issue is highlighted e.g. in EUROPEAN COMMISSION. Commision staff working document: Advancing the Internet of Things in Europe Accompanying the document Digitising European Industry Reaping the full benefits of a Digital Single Market {COM(2016) 180 final}. In: *EUR-Lex* [online]. 19. 4. 2016 [2017-10-01]. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN>, p. 22 and also discussed in the research regarding standardisation and certification of IoT, see LEVERETT, É., CLAYTON, R., ANDERSON, R. Standardisation and Certification of the "Internet of Things". In: *WEIS 2017* [online]. 2017 [2017-11-11]. Available at: <https://www.conpolicy.de/en/news-detail/standardization-and-certification-of-the-internet-of-things/>, p. 9-10. For a discussion of product liability in IoT under the US law perspective see e.g. BUTLER, A. Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices? In: *SSRN Scholarly Paper. Rochester, NY: Social Science Research Network* [online]. 2017 [2017-11-11]. Available at: <https://papers.ssrn.com/abstract=2955317>.

[119] Most economic segments are regulated in some aspect on the European or national level. Sector-specific regulation with relevant general cybersecurity requirements or implications can be found in the field of electronic communications, media, legal services, accounting, medical services, pharmaceutical industry, financial services, software, administration of critical or important infrastructure, procurement of public utilities, e-commerce etc.

[120] BACHLECHNER, D. et al. IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht. In: *Bundesministerium für Wirschaft und Energie* [online]. 2016 [2017-12-09]. Available at: <http://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf;jsessionid=D0C8D58C4B07532B65334E42E238FFF8?__blob=publicationFile&v=4>, p. 101.

[121] BACHLECHNER, D. et al. *IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht,* p. 23.

With the expansion of IoT uses in the business environment, there are considerations of possible security certification for IoT products.[122] The recently presented report by Anderson, Leverett and Clayton from the research for the European Commission on readjustment of safety regulation with regard to IoT[123] provides a deep insight into opportunities as well as limitations of regulation and standards setting for this new technology. A great deal can be adopted from the established practices in the software industry, particularly the regular vulnerability and penetration testing, following standards like ISO/IEC 29147 or ISO/IEC 30111.[124] There is need for coordinated approach to the collection and sharing of data about vulnerabilities, in-depth monitoring and coordinated response to attacks or malware infections.[125] Similar recommendations come from ENISA with regard to cybersecurity of ICS/SCAD[126] systems.[127] The need for such recommendations is bound to the increased connectivity of these previously isolated industrial systems through the adoption of IoT devices and transformation towards digital economy.

European Union is actively managing the development of the emerging IoT economy, particularly through the Large-scale pilots[128] and support to industry developed innovative solutions. It is also monitoring the process by standard developing organisations regarding IoT and cybersecurity.[129] The formulation of adequate security framework for 'Industry 4.0' is also pursued by state sponsored research groups[130] as well as by business consortia.[131] From the perspective of SMEs the self-regulatory business organisations pursuing

[122] EUROPEAN COMMISSION. Commision staff working document: Advancing the Internet of Things in Europe Accompanying the document Digitising European Industry Reaping the full benefits of a Digital Single Market {COM(2016) 180 final}, pp. 30–31. Certification is also promoted by ENISA, see INFINEON – NXP – STMICROELECTRONICS – ENISA. Common Position On Cybersecurity. In: *Enisa* [online]. 2016 [2017-12-09]. Available at: < https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity>, p. 2.

[123] LEVERETT, É., CLAYTON, R., ANDERSON, R. *Standardisation and Certification of the "Internet of Things"*.

[124] LEVERETT, É., CLAYTON, R., ANDERSON, R. *Standardisation and Certification of the "Internet of Things"*. pp. 12–14.

[125] LEVERETT, É., CLAYTON, R., ANDERSON, R. *Standardisation and Certification of the "Internet of Things"*, pp. 17–18.

[126] Industrial Control System/ Supervisory Control and Data Acquisition are terms for industrial level operational systems and architectures.

[127] ENISA. Communication network dependencies for ICS/SCADA Systems. In: *Enisa* [online]. 2016 [2017-12-09]. Available at: < https://www.enisa.europa.eu/publications/ics-scada-dependencies>.

[128] EUROPEAN COMMISSION. Horizon 2020 Work Programme 2016–2017: Internet Of Things Large Scale Pilots. In: *Digital Single Market* [online]. 2015 [2017-12-09]. Available at: <https://ec.europa.eu/digital-single-market/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots>.

[129] CEN, ETSI, IEEE, ISO/IEC, IETF, ITU and other. For detailed report see DIRECTORATE-GENERAL FOR INTERNAL MARKET, INDUSTRY, ENTREPRENEURSHIP AND SMES. Rolling Plan for ICT Standardisation 2017. In: *European Commission* [online]. 2017 [2017-12-09]. Available at: <http://ec.europa.eu/information_society/newsroom/image/document/2017-13/grow_rolling_plan_ict_2017_web_170302_C7EC62EB-0196-6C12-45229D71D00B0D6B_43894.pdf>, p. 25-32.

[130] The already mentioned German study for the Federal Ministry of Economy and Energy is a great example. See BACHLECHNER, D. et al. *IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht.*

[131] E.g. the Industrial Internet Consortium that recently published first report on its progress towards common security framework. See INDUSTRIAL INTERNET CONSORTIUM. Industrial Internet of Things Volume G4: Security Framework. In: *Industrial Internet Consortium* [online]. 26. 9. 2016 [2017-12-09]. Available at: <http://www.iiconsortium.org/IISF.htm>.

common standards often succumb to the market forces, limiting the influence of SMEs and neglecting their specific role. This makes state sponsored research with adequate participation of SMEs particularly important.

IV. 3 State Perspective – Cybersecurity and Protection against Cybercrime

The primary focus of the state coordinated assets in cybersecurity is the protection against cybercrime and cyber warfare. The legal frameworks in the EU for the combat against cybercrime are largely building upon the Budapest Convention on Cybercrime,[132] an international treaty drawn up under auspices of Council of Europe and adopted in 2001. It was by now ratified by 52 states,[133] making it crucial part of international cooperation dealing with cybercrime. The aim of the treaty is primarily the pursuit of common criminal policy against cybercrime.[134] While setting important founding stones for harmonisation of legislation and co-operation, the cybercrimes defined in the convention reflect the time of early internet. The forms of cyberattack that are most prevalent today are mostly not encompassed, particularly the ransomware or botnet infection.[135] The principles and objectives of the convention served as a base for the following progress on EU cybercrime legislation.[136] ENISA was established in 2004 to ensure high and effective level of network and information security in the EU and help develop a culture of network and information security.[137] This was followed by cybersecurity strategies[138] at the EU level and process towards adoption of network and information security directive. The NIS Directive 2016/1148[139] was adopted on 17th May 2016[140] and the member states have to implement it until 9th May 2018.[141] The directive represents first EU-wide legislation on cybersecu-

[132] Council of Europe Convention on Cybercrime, CETS 185, Budapest, 2001.

[133] Besides the EU member states are significant signatories the United States, Canada, Israel or Japan. Notable non-signatories are Russia, China, India and Brazil, which significantly limits the effect of the treaty in the global cyberspace. See Chart of signatures and ratifications of Treaty 185. In: *Council of Europe* [online]. 10. 3. 2017 [2017-12-09]. Available at: <http://www.coe.int/web/conventions/full-list>.

[134] Preamble to the Budapest Convention on Cybercrime.

[135] WEBER, R. H. *Cybersecurity in the Internet of Things: Legal aspects*, p. 723.

[136] CLOUGH, J. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*. 2014, Vol. 40, No. 3, pp. 700–701.

[137] Art. 1(1) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

[138] EUROPEAN COMMISSION. Communication: A strategy for a Secure Information Society. In: *Digital Single Market* [online]. 31. 5. 2006 [2017-12-09]. Available at: <https://ec.europa.eu/digital-single-market/en/news/communication-strategy-secure-information-society> and EUROPEAN COMMISSION. Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace. In: *Digital Single Market* [online]. 2. 7. 2013 [2017-12-09]. Available at: <https://ec.europa.eu/digital-single-market/en/news/communi-cation-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>.

[139] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

[140] EUROPEAN COUNCIL. EU-wide cybersecurity rules adopted by the Council. In: *European Council* [online]. 17. 5. 2016 [2017-12-09]. Available at: <http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/>.

[141] Art 25 NIS Directive.

rity,[142] which should promote effective cooperation and achieve high common level of protection within the EU.[143] This legislation has wide reaching effects on national cybersecurity legislation and organisation of national CSIRT units and their cooperation within the EU. The SMEs are, however, in most cases not participating on operating of the critical infrastructure and their exposure to cybersecurity law following the implementation of NIS Directive is likely to stay peripheral. The directive is adding to most national legislations two new categories of recipients.

First are the operators or essential services.[144] These services are generally defined as essential for the maintenance of critical societal or economic activity, based on network and information systems and with significant disruptive effect in case of cyber incident.[145] The particular set of recipients will differ in each member state, but the entities falling under the scope of this article are to be from sectors like energy, transportation, financial or health.[146] Given that the disruptive effect needs to be significant,[147] it is primarily encompassing large enterprises, not SMEs. However, if a SME falls into this category, it will have obligation to *"(…) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations."*[148] It shall also have further obligations to minimise the impact of eventual cyber incident and notify without undue delay the CSIRT or other competent authority about significant incident.[149] It is worth noticing that these obligations basically mirror the structure of obligations of any data controller or processor with regard to data security and data breach under the GDPR, even though the purpose, framework and competent regulatory authority understandably differ considerably. The second group includes digital service providers,[150] specifically providers of online marketplace, online search engine or cloud computing service.[151] Even this category is unlikely to encompass SMEs, but even if then the only obligation under the NIS Directive for these entities is cyber incident notification in case of a substantial impact on the provision of the service.[152]

SMEs are therefore more likely to be affected by general national cybersecurity policies or specific measures taken in response to widespread cyberattacks. Some SMEs may be subject to specific obligations under national law, particularly if they supply services to public administration or operate important information infrastructure, but the majority of SMEs stay under the radar of this type of legislation. Nonetheless, the aggregate role of SMEs in

[142] EUROPEAN COMMISSION. Network and Information Security Directive: co-legislators agree on the first EU-wide legislation on cybersecurity. In: *Digital Single Market* [online]. 12. 9. 2015 [2017-12-09]. Available at: <https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation>.
[143] Art. 1(1) NIS Directive.
[144] Art. 5 NIS Directive.
[145] Art. 5(2) NIS Directive.
[146] Annex II. to NIS Directive.
[147] Particular criteria are based on Art. 6 NIS Directive.
[148] Art. 14(1) NIS Directive.
[149] Art. 14 (2,3) NIS Directive.
[150] Art. 4(5) NIS Directive.
[151] Annex III. to NIS Directive.
[152] Art. 16(3) NIS Directive.

the emerging digital economy is likely to remain significant and with the spread of IoT adoption, there may be need for more broadly coordinated cybersecurity efforts including SMEs.

V. DISCUSSION

The aim of this paper is to highlight a particular challenge that the digital economy is likely to have on SMEs. The spread of IoT devices interacting with their corporate networks will likely mean more frequent and more damaging cybersecurity threats. The SMEs possess particular features that make them likely victims of cybercrime and that limit their capacity for adequate cybersecurity. Furthermore, the increased attention devoted to cybersecurity on the side of primary cybercrime targets[153] may further add to the pressure on SMEs. This is in the economic literature described as negative spill-over effect.[154] Cybersecurity is largely a game of chasing the weakest link leading to the richest bounty and SMEs end up being increasingly popular targets in this regard.

Given the particular features of cyber incident cost distribution, there may often be lack of incentive for the SME to invest into cybersecurity and prevent an event that takes a form of negative externality, given that the victim is remote and unrelated and the damage is often intangible and ambiguous. This deformity of cybersecurity risk distribution has features of market failure,[155] as the externality of incurred costs limits the demand for secure solutions by entities that need to implement them.[156] The SMEs stand in this regard on various positions of the failing equation. They may be the producer that is not motivated to develop a product with security by design in mind. They may be the provider of service that does not value adequately the risk of data breach or addition to botnet for DDoS attack on critical infrastructure. They may also be the victim that relied on weak security solution or which assets became target of cybercrime. This versatility, together with their significance for innovation, employment and economic growth, makes SMEs a particularly demonstrative category for analysis of cybersecurity challenges presented by new technologies. Their capacity to deal with the challenges is limited by default through their budget, headcount or know-how. Cybersecurity often takes low priority in the perception of the SME executives and owners, as they assume that the enterprise holds no valuable assets compared to larger entities. There is broad adoption of so called "security by obscurity" approach.[157]

---

[153] Reports indicate increasing cybersecurity investment, particularly by large entities or components of critical infrastructure. E.g. CYBERSECURITY INSIDERS. 2017 Cybersecurity Trends Report. In: *Cybersecurity Insiders* [online]. [2017-11-11]. Available at: <https://www.cybersecurity-insiders.com/portfolio/cybersecurity-trends-report/>; or PWC. Global State of Information Security® Survey 2017. In: *PWC* [online]. 2017 [2017-11-11]. Available at: < https://www.pwc.com/us/en/cybersecurity/information-security-survey.html>.

[154] KOBAYASHI, B. Private versus social incentives in cybersecurity: Law and economics. In: *The Law and Economics of Cybersecurity* [online]. 2005. [2017-12-09] Available at: <https://www.researchgate.net/publication/289775072_Private_versus_social_incentives_in_cybersecurity_Law_and_economics>, pp. 26 et seq.

[155] INFINEON – NXP – STMICROELECTRONICS – ENISA. *Common Position On Cybersecurity*, p. 1.

[156] CLARKE, R. *The prospects of easier security for small organisations and consumers*. pp. 544 et seq.

[157] GRONER, R., BRUNE, P. Towards an Empirical Examination of IT Security Infrastructures in SME. In: *Nordic Conference on Secure IT Systems*: *Secure IT Systems* [online]. 2012 [2017-12-09]. Available at: <https://link.springer.com/chapter/10.1007/978-3-642-34210-3_6>.

As indicated in the previous chapter, there is no lack of regulatory frameworks creating obligations for entities including SMEs with regard to cybersecurity measures. Yet the real challenge the entities are facing with regard to these obligations is in their complexity. Even if the SME management is aware and vary of the risks it is facing, there is great uncertainty about the proper approach and adequate measures to be taken to comply with the regulation and to achieve an appropriate level of security. The labyrinthine requirements included across various legislative frameworks discourage adequate compliance, particularly if the recipient is microenterprise with few employees, limited cybersecurity know-how, primary focus in unrelated field and numerous other administrative and regulatory obligations to cope with.

Standage in his recent article offers a great lesson that can be learned about cybersecurity from maybe the first 'hack' of communication. The story is about Blanc brothers, exchange traders from Bordeaux, who modified the early mechanical telegraph messages between 1834 and 1836. They hacked the system by bribing the operators. There are many parallels that the article aptly draws to the current state of cybersecurity. It is mostly the human failing not technological vulnerability that is the weakest link of the system or network. At the same time, it is naïve to hope for technological solution to this weakness. Rather than attempting impenetrable systems, resiliency, awareness, understanding and adaptability are the way forward is cybersecurity. After all, the malicious activities are here with us to stay, as they are part of human nature.[158]

The upcoming boom of IoT devices is likely to raise the stakes higher and further stress the capacities of SMEs to achieve needed measures. The growingly diverse technological dimension of the issue will bring new challenges through transformation of the role and scope of ICT in the SME business operations. It is not that cybersecurity can be made perfectly impenetrable with any system of measures or for any amount of investment, as it generally follows a function of diminishing returns,[159] but a minimal level of protection must be achieved and this cannot be directly bound to optimization of implementation costs, as otherwise the requirement misses its purpose. The actual adequate application of cybersecurity principles and measures is generally based on rather practical approach to achievable solutions,[160] however, limited understanding, confusing guidelines and fragmented best practices often creates obstacles for recipients without expert knowledge.[161]

The challenge of regulation in the field of SME cybersecurity is similar to the challenge in most areas related to the cyberspace or new technologies. Given the fast changing technology landscape, any regulatory approach is faced with the "pacing problem".[162] The most flexible regulation can be provided by self-regulatory frameworks, these, however, tend to

[158] STANDAGE, T. Rewind: The crooked timber of humanity. In: *The Economist 1843* [online]. 2017 [2017-12-09]. Available at: <https://www.1843magazine.com/technology/rewind/the-crooked-timber-of-humanity>.

[159] See GORDON, L., LOEB, M. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*. 2002, Vol. 5, No. 4, p. 445.

[160] A great practical guide in this regard was provided by CRUME, J. *Inside Internet Security: What Hackers Don't Want You To Know*. Addison-Wesley Professional, 2000.

[161] CLARKE, R. *The prospects of easier security for small organisations and consumers*, p. 539.

[162] MARCHANT, G. E., ALLENBY, B. R., HERKERT, eds. *The Growing Gap Between Emerging Technologies and Legal Ethical Oversight*. Springer, 2011, p. 7.

succumb to the rules of market forces.[163] The public authority therefore needs to set and supervise regulatory regime with regard to the externalities that the self-regulatory approach generates. GDPR as well as the NIS directive exemplify an active pursuit of this goal. The hype around their implementation provides a rare window of increased attention to cybersecurity measures by many, including the SMEs. This opportunity should be seized to send a message about the importance of cybersecurity for SMEs not only in current settings, but particularly in face of upcoming advances in ICT development.[164]

The SMEs need to be guided through the complexity of the issue and clearly communicated the added value of the required measures. The awareness needs to be heightened to the threats related to IoT connectivity, but particularly to the solutions and best practices that allow the implementation of these devices in the business operations of SMEs. The cybersecurity or data protection requirements need to be implemented in a fashion that does not add to the difficulty of doing business for the SMEs. A combination of understandable guidelines,[165] encouraging stimuli[166] and restrained sanctions following timely security audit[167] can prepare the European SMEs for the era of IoT. Failure or hold-up of this process may on the other hand give rise to additional obstacles to doing business and aggravate the negative impact of connectivity in the emerging Single digital market.

VI. CONCLUSION

There current development in the EU indicates a growing awareness to the issues of cybersecurity and data protection. The role and specific position of SMEs is to a large degree recognized, but IoT should be perceived with greater attention to the particular effects on the SMEs capacity of doing business. Further development of guidelines and support tools should be encouraged in order to provide the SMEs with better understanding of their obligations and their purpose in the interconnected data economy.

[163] CLARKE, R. *The prospects of easier security for small organisations and consumers*. p. 544.

[164] INFINEON – NXP – STMICROELECTRONICS – ENISA. *Common Position On Cybersecurity*, p. 3.

[165] INFINEON – NXP – STMICROELECTRONICS – ENISA. *Common Position On Cybersecurity*, p. 2. The previously mentioned guidelines for SMEs with regard to obligations under GDPR exemplify this form of support. See ENISA. *Guidelines for SMEs on the security of personal data processing*.

[166] CLARKE, R. *The prospects of easier security for small organisations and consumers*, p. 544. The stimulatory measures include particularly support of research like the above mentioned LEVERETT, E., CLAYTON, R., ANDERSON, R. *Standardisation and Certification of the 'Internet of Things'*. Also awareness campaigns, like European Cyber Security Month, help focus the attention in the right direction. See ENISA. European Cyber Security Month. In: *Enisa* [online]. [2017-10-02]. Available at: <https://cybersecuritymonth.eu/>.

[167] The need for timely audit as precondition for effective incentive by non-compliance sanction is highlighted e.g. by LAUBE, S., BÖHME, R. The Economics of Mandatory Security Breach Reporting to Authorities. *Journal of Cybersecurity*. 2016, Vol. 2, No. 1, [2017-10-10]. Available at: <http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf>.