DIGITAL ECONOMY AND INDUSTRY 4.0

Petr Doucek, Jiri Holoska

Faculty of Informatics and Statistics
University of Economics, Prague
doucek@vse.cz, jiri.holoska@vse.cz

Keywords

Digital economy, industry 4.0, Internet of Things, cyber security, cyber security risks

Abstract

The development and penetration of information technologies (IT) into our everyday life changes the paradigm of entire society. The impact of IT integration on our life is reflected both in how we use information technologies and in society's ethics. However, expected positive effects, such as higher labor productivity, the elimination of routine work, better control, etc., come with limitations and risks. This article points out some aspects of the security of devices that constitute an integral part of the Industry 4.0 concept. Security gaps are especially in remote access to such devices, the use of communication protocols with lower security and the way passwords in text form are stored.

1 Introduction

The development of information and communication technologies (ICT) significantly impacts the further development of our globalized society. The bigger the impact and influence on entire human society is, the more information technologies become its integral part (Teplý, Kvapilíková, 2017). Some thoughts about the inseparability of information technologies from human society have already been presented e.g. in Carr's elaboration (2004) where the author compares the use of ICT in organizations' utilities and the overall impact of ICT on the economy to the industrial revolution's phases – steam in the 19th century, electricity in the 20th century (Kelly, 1998). ICT become a necessity for modern, dynamic activities of society that finds itself at a stage of major changes. When looking at the development of the past 20 years, it is obvious that the economy's dynamics fluctuate and that high expectations are put on ICT that are supposed to resolve, or at least considerably help to resolve, society's problems (Basl, Sasiadek, 2017).

The current transformation caused by a massive onset of digitalization includes practically all areas of the economy and social life (Basl, 2017). The main approaches and trends concerning industrial production and its links are available e.g. in (Basl, Doucek, 2019). Research on the impact of information technologies on the development of net production and thus on the environment and the concept of permanently sustainable development or sustainable development is another important trend (Bruntlandová, 1991).

This trend is connected to the social responsibility of both organizations and individuals. In the current closed system of finite resources of a globalized society, organizations contribute, by being

socially responsible, to sustainable development, [1] to a balance between three basic interconnected areas of life and to sustainable development (Figure 1), thus jointly representing a certain model as well as a vision of society's development.

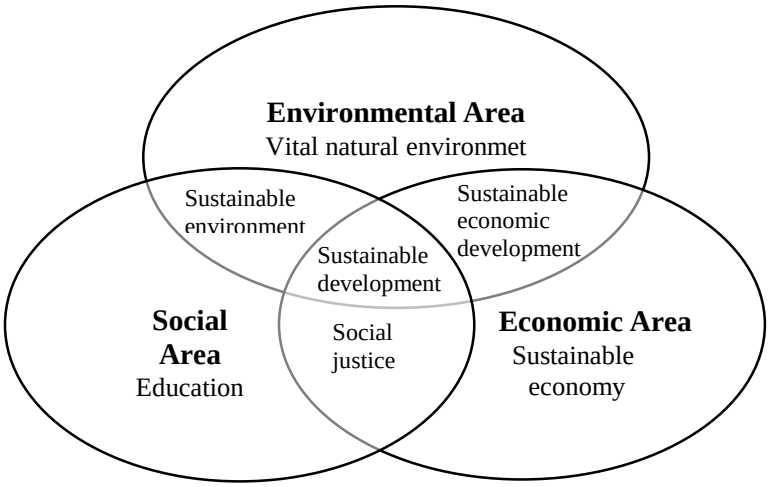

Figure 1: The intersection of the basic pillars of Corporate Social Responsibility and Sustainable Development (Moon, 2010)

The basic pillars of social responsibility and sustainable development are as follows:

- **Economic growth** – businesses should be transparent and have a positive relationship to investors, customers, suppliers and other business partners, and the impact on the regional, national and global economy should be monitored, including employment development and the fight against corruption;
- **Environment** (a sustainable natural balance) – organizations realize their impact on the environment and its ecosystems (water, land, air) and their activities will thus burden the environment as little as possible;
- **Social area** (social progress) – this includes an approach to own employees in terms of living standard, health, safety, education, cultural development and regional development support in these areas.

This trend, nowadays reflected by attempts to influence the environmental development and to galvanize society to protect the environment, represents a space and opportunity for applying information technologies.

Potential threats and limitations of used and implemented information technologies lie in the functioning of information systems. We all can surely imagine a failure of the systems that concern our everyday life – from banking systems, to local, long-distance and transcontinental transport control systems all the way to strategic and air defense systems. We have been bedazzled by ICT possibilities for some time now, but let's look at real ICT threats and limitations. The areas presented

[1] The first definition of sustainable development from the Report for the UN World Commission on Environment and Development (WCED) called "*Our Common Future*" and presented in 1987 by former Norwegian Prime Minister Gro Harlem Brundtland says: "Permanently" sustainable development is such development that meets the needs of the present without compromising the ability of future generations to meet their own needs." (Brundtland, 1991).

below are very closely connected. The first one concerns the maturity of people operating information systems – their ethics. (Sigmund, 2014, 2015) Security is another area.

In this article, we would like to also present the risks of a blanket use of information technologies, e.g. in the form of Internet of Things.

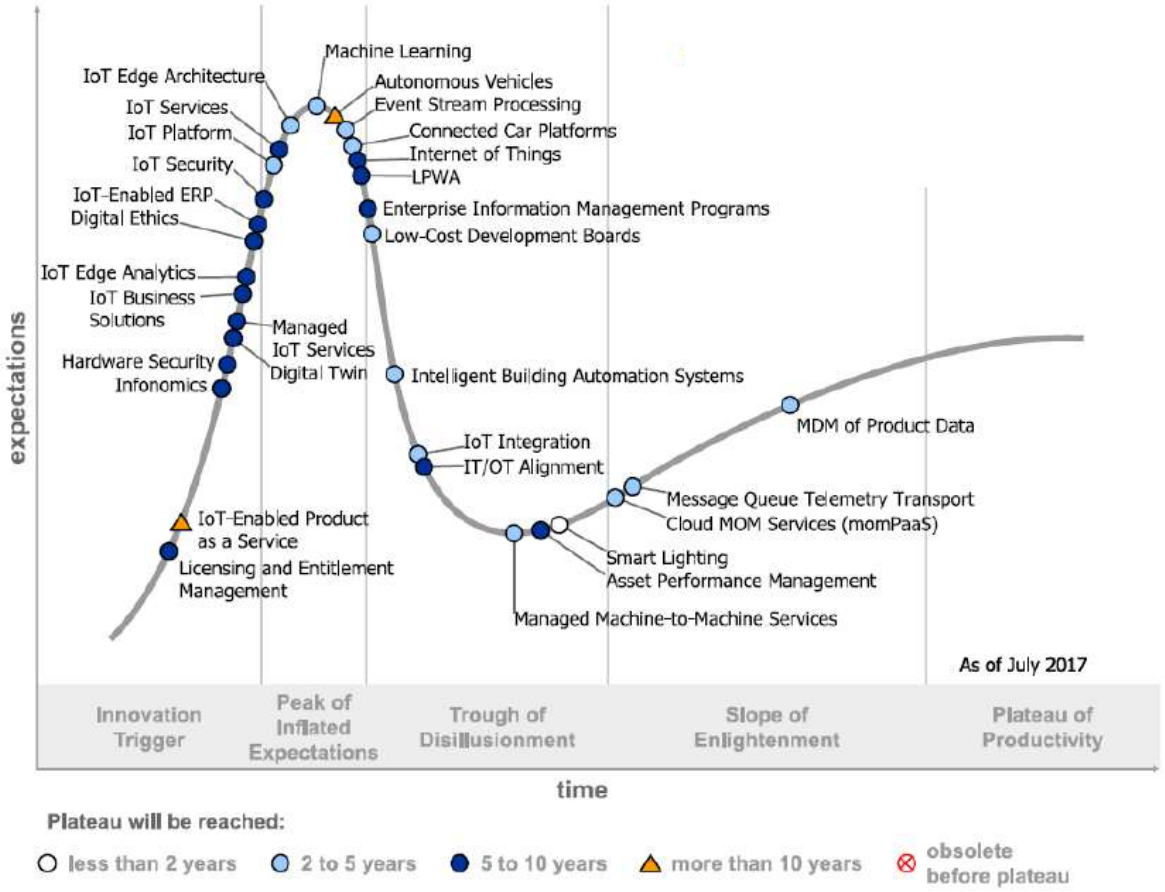

Figure 2: Hype Curve for Internet of Things 2016 (Gartner, 2016)

Marik describes the concept of security of Industry 4.0 applications (2016):"The safety and reliability of Industry 4.0 systems must be understood in a comprehensively systematic way — from data and communication security at the lowest level, on through infrastructure reliability and security, on out to global system security at the level of manufacturing plants or chains of them, including the upholding of individuals' information privacy and of intellectual property rights."

Such defined cyber risks represent a new challenge but also new limitations with which we will have to deal in the future when implementing ICT. The most common risks that we usually deal with concern information technologies – the time of their operation, reliability – i.e. their technological aspect.

This is also proven by the fact that security risks of Industry 4.0 are often discussed. These risks usually stem from the wireless transmission of data between production and monitoring devices and their sensors that implement the idea of Industrial Internet of Things (IIoT). This usually concerns the hacking of this type of connection or device or a potential interference due to the operation of other electronic and electric devices. A rather important aspect of processed data is the complexity of their security (Marik, 2016). This is about ensuring the integrity of transmitted and processed data. This fact considerably affects the reliability and completeness of provided data collected through sensors and stored in data warehouses or lakes. Providers try to ensure full data integrity that cannot

be compromised in any way during data transmission. The limit here is set up in a way that if we receive data that are somehow distorted (a defective sensor, a wrong temperature measurement – e.g. the sensor sensitivity is lower than required, the sensor is worn out due to the environment or measurements are wrong due to a low battery voltage), the automated control system with fixed required values then directs the controlled system in the wrong direction. This factor may lead to false (inaccurate, detached from reality) virtual reality – a digital image of the controlled system where information flows will not display actual material or energy flows. Control based only on data from sensors may lead to loss of confidence in information systems that monitor real phenomena through censors as well as in the data stored in these systems. The use of artificial intelligence elements without effective control by man may destroy the entire controlled system. As an example, we could mention two fatal Boeing plane crashes.

According to Marik (2016), a more comprehensive concept of security in Industry 4.0 is based on taxonomy as mentioned in Lezzi's Lezzi, Lazoi, Corallo, elaboration (2018). Here, cybersecurity with respect to Industry 4.0 is considered a unity of systematic vulnerability, cyber threats, from which arise risks and measures adopted to protect company assets. Another matter that organizations must deal with in connection to security in cyberspace is the cybersecurity management system. They must apply best practices in the form of guidelines for implementing cybersecurity reference models (Novák, Doucek, 2018) and propose and implement countermeasures in the form of security projects (Novák, Doucek, 2017).

Another and completely different security dimension includes comprehensive protection of a company information system as a whole and company assets through the functions of the information security management system (ISMS). It still holds true that the security of the entire information system of a company is as strong or weak as its weakest link.

2 Methodology

The fundamental approach to collecting data used in this article is that of studying subject literature and comparing the founded facts, both among each other and with our mental models in the area of security in Industry 4.0 and digital economy, the circular economy included. Added value of this article is that it does not promote the information technology but it also presents the dark sides of it in business and every day´s life.

The results of our research could fill up many pages, but in this article, we would like to focus only on the risks of IoT implementation in small and medium-sized businesses (van Kranenburg, 2018). According to Flatt, Schriegel, Jasperneite, Trsek, Adamczyk (2016) typical threats for cyberattacks are:

- Direct attacks on external accesses;
- Indirect attacks on the IT systems of the service provider for which the external access has been granted;
- Unknown attack vectors without detection capabilities enabled by unknown vulnerabilities (or zero-day exploits);
- Non-targeted malicious software which infects components and impairs in their functionality;
- Intrusion into neighbouring networks or network segments (for instance, the existing office network).

In our article we will focus on potential direct external attacks on select devices. According to McAfee (Wineberg, 2015) the number of attacks on IoT devices will go up considerably. It is because the number of these devices will increase, they will be less secured and, last but not least, the data generated on such devices will be important.

3 Results

Why are we focusing on SMEs? Large and transnational companies have large teams of specialists in information technologies, communication, security, system architecture, network elements, administration aspects, data storing and processing and many other matters. Small and medium-sized businesses, especially micro firms, cannot hire highly specialized professionals mainly for financial reasons and thus the risk of increased and potent cyber threats due to the implementation of IoT elements in their information systems is much higher and will have a much more important impact on these systems.

One of the main technology-oriented results concerning IoT security is the identification of threats that may impact the functionality of company information systems through the integration of sensors and data that are recorded and transmitted by these sensors. These company information systems typically include different types of internet cameras, thermostats or sensors on production lines. The method of transmission of data from standard commercial devices is often attacked by hackers.

What are IoT, automation and smart devices: Electronic devices designed to perform specific tasks and operate within other devices or management systems with scope multiple technology fields from automation on assembly lines to the smart sensors and devices for home use. Current challenges of IoT devices are mainly:

- Power consumption is one of the concerns when deploying variety of electronic device within enterprise or at home.
- Low power consumption system on chip (SOC) requirements define computational and processing resources of small CPUs unites, that are not capable electively handle processing overhead introduced with strong end-to-end encryption and authentication schemes.

The most common IoT implemented devices are different types of sensors, smart cameras, thermostats big data, etc. Primary security concern on the default IoT use case, smart sensors or data generating device, smart IP cameras included are meant to be available 24/7 sending data either to on-premise server, but primarily to vendor cloud environments. In order to connect to the cloud environment, the internet access is required, very often are smart IoT devices exposed directly to internet on public IP address space that translates to condition where the device security relies on proper configuration and firmware security. Smart devices may hold more then one network interface let it be, Ethernet and Wi-Fi or Broadband 3G / 4G mobile internet connectivity. **Network exposure is a critical element to the IoT security from perspective of entry point the technology solution which smart devices are part of**. Exposed configuration / management web portals, ssh or even telnet services or exposed communication bus interfaces, Onboard Data Port – car hacking.

The following text will focus on a potential direct attack.

SMEs very often use internet cameras and thermostats (Wineberg, 2015). Their connection to a computer network comes with the following risks in particular. The main identified risk in the case of cameras is:

- The backup of information about login passwords in text form;

- The use of the protocol http and not https for communication; the use of this protocol in some devices is optional;
- The use of User Datagram Protocol for communication with users.

Identified weaknesses in the case of thermostats are very similar:

- The use of the protocol http and https or only the protocol http for communication.
- Open wifi for initial pairing.
- No certified pinning.

4 Conslusion

The Industry 4.0 concept and the follow-up concept of digital economy and the massive implementation of artificial intelligence in business models (Maryska, Doucek, Sládek, Nedomova, 2019) and thus in everyday life changes the paradigm of society's functioning. Up until now we did not fully understand the growing dependency of people from Western society on information technologies (Teplý, Klinger, 2018). However, this dependency will become critical for our civilization after the implementation of data-collecting sensors and follow-up structures of data stored in cloud technologies and distributed in the computer networks practically of the entire planet. This dependency will be critical not only in terms of technologies but also in terms of ethics – who will have the right to monitor practically anything about people and to evaluate and make decisions based on these data – morality and the system of civil and life values.

The Industry 4.0 concept and follow-up innovations do not only change the level of implementation of information technologies but also society as a whole, including its fundamental values. Only an integral development of technologies and human values is able to ensure a harmonious society in the future.

5 Acknowledgement

Paper was processed with contribution of the Czech Science Foundation project GAČR 17-02509S and with support from institutional-support fund for long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the University of Economics, Prague (IP400040).

6 References

Basl, J. (2017). Penetration of Industry 4.0 Principles into ERP Vendors' Products and Services – A Central European Study. Proceedings of the International Conference on Research and Practical Issues of Enterprise Information Systems. DOI: http://dx.doi.org/10.1007/978-3-319-94845-4_8

Basl, J., & Sasiadek, M. (2017). Comparison of Industry 4.0 Application Rate in Selected Polish and Czech Companies. Proceedings of the International Conference IDIMT-2017 Digitalization in Management, Society and Economy. Available at: http://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2017.pdf

Basl, J., & Doucek, P. (2019). A Metamodel for Evaluating Enterprise Readiness in the Context of Industry 4.0. Information, 10(3). DOI: http://dx.doi.org/10.3390/info10030089.

Bruntlandová, G. H. (ed.). (1991). Naše společná budoucnost. Praha: Academia, 1991, ISBN 80-85368-07-2

Carr, N.G. (2004). Does IT Matter? Information Technology and the Corrosion of Competitive Advantage. United States, Harvard Business School Press, 2004, ISBN 1-59139-444-9

Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016). Analysis of the Cyber-Security of Industry 4.0 Technologies based on RAMI 4.0 and Identification of Requirements. Proceedings of the 21st IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). DOI: http://dx.doi.org/10.1109/ETFA.2016.7733634

Gartner (2016). Hype Cycle for the Internet of Things 2016. Available at: https://www.gartner.com/document/3371743

Kelly, K. (1998). New Rules for the New Economy, Ten Radical Strategies for the Connected World. Penguin Group, New York USA, 1998, ISBN 067088111-2

Lezzi, Marianna & Lazoi, Mariangela & Corallo, Angelo. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry. 103, 97-110. DOI: http://dx.doi.org/10.1016/j.compind.2018.09.004.

Marik V. (2016). Průmysl 4.0 Výzva pro Českou republiku. Management Press: Prague, Czech Republic, 2016, ISBN 978-80-7261-440-0

Maryska, M., Doucek, P., Sládek, P., &Nedomova, L. (2019). Economic Efficiency of the Internet of Things Solution in the Energy Industry: A Very High Voltage Frosting Case Study. Energies. 12(4). DOI: http://dx.doi.org/10.3390/en12040585.

Moon, Y., B. (2010). Syracuse University USA, keynote on the conference CONFENIS 2010, Natal, Brazil.

Novák, L., & Doucek, P. (2018). Personal Data Protection in Cyber Space. Proceedings of the International Conference IDIMT-2018 Strategic Modeling in Management, Economy and Society. Available at: https://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2018.pdf

Novák, L., & Doucek, P. (2017). Regulation of Cyber Security in the Banking Sector. Proceedings of the International Conference IDIMT-2017 Digitalization in Management, Society and Economy. Available at: http://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2017.pdf

Sigmund, T. (2015). Do We Need Information Ethics? Proceedings of the International Conference IDIMT-2015 Information Technology and Society Interaction and Interdependence. Available at: http://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2015.pdf

Sigmund, T. (2014). Privacy in the Information Society: How to Deal with its Ambiguity? Proceedings of the International Conference IDIMT-2014 Networking Societies – Cooperation and Conflict. Available at: http://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2014.pdf

Teplý, P., & Klinger, T. (2018). Agent-based modeling of systemic risk in the European banking sector. Journal of Economic Interaction and Coordination, DOI: https://doi.org/10.1007/s11403-018-0226-7

Teplý, P., & Kvapilíková, I. (2017). Measuring systemic risk of the US banking sector in time-frequency domain. The North American Journal of Economics and Finance. 42, 461–472. DOI: http://dx.doi.org/10.1016/j.najef.2017.08.007.

van Kranenburg, R. (2018). The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID. Netherlands, Institute of Network Cultures: Amsterdam, 2008, ISBN 978-90-78146-06-3.

Wineberg, W. (2015). Hacking 14 IoT Devices. Available at: https://www.iotvillage.org/slides_DC23/IoT11-slides.pdf