CZESTOCHOWA UNIVERSITY OF TECHNOLOGY

FACULTY OF MANAGEMENT

Ph. D. dissertation

INFORMATION SECURITY MANAGEMENT AT UNIVERSITIES

Author: mgr Grzegorz Chmielarz

Supervisor: Dr hab. inż. Robert Kucęba, prof. PCz

Częstochowa 2018

Currently, functioning of organisations is to a large extent based on their use in the operations the global network – the Internet. The development of the functionality of the Internet has caused the changes not only in the environment that the contemporary organisations operate in. Its measurable consequence is also the common assess to the global network and growth of interest in making use of its advantages in the conducted business activity[232]. Moreover, it has to be stressed that the change of the mode in which both individual users as well as economic entities function in the digital reality is an outcome of the development of Information Society, which is defined as new social, economic and cultural phenomena that originated in the second half of the XX century as a result of information technologies influence"[233]. The concept of Information Society concerns technical tools of communication, storing and transforming information. Its characteristic features include[234]:

- highly developed service sectors, mainly modern services sector, which includes banking, finances, telecommunication, informatics, research, development and management. In some countries this sector provides employment for over 80% of professionally active population, and the traditional services sector exceeds slightly 10%;
- knowledge based economy;
- high level of society's enrolment;
- ongoing process of society decentralisation;
- local society renaissance;
- social life enrichment.

Common, unlimited access to the Internet in the Information Society and implementing modern methods and tools of data processing are the reason behind tremendous amount of data being generated currently. Personal data and information of private nature are being processed nowadays on an unprecedented scale. For example, currently in just two days as much data is being produced as the mankind produced until 2003[235]. Therefore, it is worth

---

[232] Jelonek D., *Przestrzeń internetowa w otoczeniu organizacji. Implikacje dla zarządzania strategicznego. Zarządzanie Strategiczne Quo Vadis?,* Prace Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości, red. R. Krupski, T. 22 (2) 3013, p. 310-311

[233] Goliński M., *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru,* Oficyna Wydawnicza SGH, Warszawa 2011, p. 31

[234] Chmielarz, W. Materiały wykładowe dostępne pod adresem: http://wz.uw.edu.pl/pracownicyFiles/id4191-ebiznes4.ppt (accessed on 26.03.2018)

[235] http://www.giodo.gov.pl/487/id_art/9146/j/pl/ (accessed on 26.04.2018)

stressing that as a consequence of information technologies development and the growth in the level they are used both in case of individual users as well as organisations, one can observe a significant growth of the amount of information and personal data, which are being processed in the information systems of contemporary organisations, which constitutes a serious challenge to ensuring their proper security level. Until recently a large number of public and private organisations were not aware of the value of information resources they had gathered, which as a result marginalised the issue of managing properly the security level of possessed information and personal data. Yet, according to the estimates the value of EU citizens personal data will amount almost 1 billion Euro per year until 2020.[236] For example, a set of all information that a credit card contains, that is its name, number, expiry date, birth date and CVV2 code (a three-digit security code placed on the back of the card) in February 2017 cost about 30-45 US dollars. Credit cards containing only the CVV2 code are available at 5 US dollars a piece. In case of credit cards repositories, where the information recorded on the magnetic strap can be copied onto empty cards, their prices range from 200 to 300 US dollars[237]. So, in case of organisations that to a large extent function in the virtual environment, whose information systems are connected permanently to the Internet, more and more often attempts of unauthorised access to private information can be observed, in this personal data, gathered and stored in the resources of their information systems. According to the data from a report by Google in the period from March 2016 to March 2017 approximately 3.3 billion of personal records found their way to the black market, and 12 million people lost their data as an outcome of phishing attacks[238]. For comparison, in the course of a decade (2004-2014) there were only 229 serious incidents of personal data security breaches in Europe[239]. Personal data breaches incidents pose a considerable threat to the activity of organisations. Therefore, it seems reasonable to implement proper legal regulations that will define the issues of managing the security of processed information and personal data in organisation. In this respect, it is worth noticing that the previously valid legislative measures in the area of information and personal data protection originated at the time when electronic media was used to much a smaller extent

[236] http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/ (accessed on 25.03.2018)

[237] http://www.krollontrack.pl/blog/2017/02/27/czarny-rynek-danych/ (accessed on 28.05.2018)

[238] http://wyborcza.pl/7,156282,22775248,raport-google-ponad-3-miliardy-danych-skradzionych-w-ciagu.html?disableRedirects=true (accessed on 28.05.2018)

[239] Howard, P. N. i Gulyas, O. (2014). *Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe*. SRN: https://ssrn.com/abstract=2554352 (accessed on 26.03.2018)

than nowadays. The oldest European legal act that regulated the issues of personal data protection was the European Council's Convention NO 108 of 28 January 1981 on Protection of Individuals with regard to Automatic Processing of Personal Data. Under the Convention the EU member states were obliged to create and implement legislative solutions that would regulate personal data protection issues. The main goal of the Convention was to protect the laws and freedom of all EU citizens, in any of its member states, regardless of their citizenship and place of residence. A particular stress in the Convention, which became effective on 1 October 1985, was placed on private persons rights to have their personal sphere respected, in this in the area of automatic personal data processing[240].

Another legal act that regulated the issues of personal data protection of EU citizens was the Directive 95/46/EC on physical persons protection with respect to personal data processing and free movement of this data issued on 24 October 1995. This Directive aimed at ensuring a minimal level of personal data protection of EU member states citizens gathered in data sets, as well as making available free movement of personal data within the member states.

However, the Directive 95/46/EC constituted a set of framework guidelines concerning the issues of information security management, which were additionally made more detailed in the internal regulations of particular member states. In case of Poland this function performed the Law on Personal Data Protection of 29 August 1997 (Dz. U.02.101.926), as amended, with the last amendment on 28 June 2016 (Dz. U. z 2016 poz. 922). The provisions of the Law introduced new standards in the scope of information and personal data protection that were processed in organisations. The Law on Personal Data Protection was also the first legal act that established an obligation to create in organisations the Security Policy – a document that specified a strategy and set of procedures aimed at securing informatic systems used for personal data processing. Creating the Security Policy was a formalisation of the processes of personal data protection in organisations and significantly contributed to an increase in the level of security of information and personal data processing in organisations.

On 25 May 2018 the new EU General Personal Data Regulation, commonly called GDPR, comes into force. It constitutes a set of guidelines for all organisations and public institutions that process personal data. All these organisations are supposed to ensure compliance of data

---

[240] http://giodo.eprace.edu.pl/480,Podstawy_prawne_ochrony_danych_osobowych.html (accessed on 25.05.2018)

processing with new legislative measures in this respect. The regulation concerns all the organisations that in the course of their activity collect, process, store, transmit or analyse personal data. As higher education institutions are a group of organisations where due to the nature of their operation personal data is processed to a relatively large extent, it is necessary that the implemented methods and tools of information and personal data security guarantee the compliance of data processing with the requirements imposed by the correct law regulations. It is also worth stressing that since 25 May 2018 the previously valid Law on Personal Data Protection has been replaced by the new Law of 10 May 2018 on Personal Data Protection (Dz. U. 2018 poz. 1000), which mainly aims at making the GDPR regulations more precise. Therefore, so as to ensure the proper security level of information and personal data management in higher education units it is necessary to determine the dependencies included in the following research problems of the present dissertation:

P.1 *What factors condition designing and implementing the information management policy in higher education institutions?*

P.2 *What relationships occur between the organisational structure of higher education institutions and their autonomous information security structure?*

P.3 *What risks occur in implementing the information security management policy and what methods should be applied to prevent their occurrence?*

With defined in this manner research problems that simultaneously determine research gaps the following **main goal (CG)** of the doctoral dissertation has been established:

Defining the information security management structure in higher education institutions considering the binary relationships between information management and procedures of their security management.

With respect to the main goal of the present dissertation and so as to enable its full achievement, the following partial goals have been defined: cognitive, empirical and project ones.

The cognitive goal C1 of the doctoral dissertation is to introduce the taxonomy of information and information security management, which has been achieved based on the literature query.

The empirical goal C2 is to conduct the analysis and assessment of information security management systems in selected higher education institutions.

The **project goal C3** of the present dissertation is to define the organisational structure of information security management in higher education institutions.

Considering the defined research problems, the main goal and detailed goals of the dissertation will be carried out on the basis of the accepted **main hypothesis HG** that assumes the following:

Information security management requires that procedures and operating tasks are adjusted to particular units in the autonomous information protection structure in the organisation.

The main hypothesis is supplemented and made more detailed by two auxiliary hypotheses that will be fully verified in the dissertation as well. These hypotheses state that::

HP 1. *Identifying information flow channels in the organisational structure is the basis for designing and implementing information security management system.*

H 2. *Autonomy of information security management reduces the risk of generating threats in the whole organisational structure*

In order to verify the main hypothesis and accompanying it auxiliary hypotheses and to achieve the research goals, empirical research has been conducted that was divided into two stages – a questionnaire and direct interview. The methods have been described and justified in detail in sub-chapter 4.1.

Achieving the main goal and detailed goals as well as verifying the main hypothesis and auxiliary hypotheses have determined the structure of the dissertation.

In particular:

in the **first chapter** the Author has presented the nature and conditionings of information management in economic entities. The chapter includes definitions of data, information and knowledge and their importance for organisations. Moreover, it also includes the presentation of structures and functionality of information management systems as well as methods and tools of information protection implemented in economic entities. The final part of the chapter introduces the portfolio of terms referring to the area of information security management.

In **the second chapter** the cognitive concentration concerned the role and importance of personal data management in organisations. First, the Author has presented in it personal

data ontology in information management systems. Then, a review of legislative restrictions in the area of personal data management in organisations has been presented and procedures of personal data management in organisations have been characterised. The chapter finishes with a presentation of personal data security policy in economic entities with reference to its strategic role.

The subject matter of the **third chapter** concentrates on information and personal data management in higher education institutions. The Author has defined in it the structure of information and data flow in higher education institutions and characterised procedures of information and personal data security management that are implemented in higher education institutions. Moreover, the chapter includes an analysis of information security management procedures in organisations and the issue of their adjustment to the specificity of higher education institutions functioning.

In the **fourth chapter** elaborated on the basis of own research the Author includes an analysis of structures and procedures of information security management in Polish higher education. Criteria of higher institutions selection for the research process have been presented in it and the research sample and research methods have been characterised as well. The chapter also includes an analysis of the questionnaire survey participants with reference to the roles that particular entities in the information management structure play in the personal data processing in higher education institutions. Additionally, the Author has conducted an analysis of the survey results aimed at determining and measuring the procedures implemented in the area of information security management in higher education institutions and defined risks occurring in this area, as well as applied methods and technologies that may reduce or eliminate them.

In the **fifth chapter,** the second empirical chapter of the dissertation, the Author presents the second stage of the empirical research conducted in the expert group, where the experts evaluated the efficiency of information resources management in the structures of higher education institutions and the influence of delegating tasks on the functions of information management in higher education institutions. Moreover, the subject of the analysis was compliance of information security management systems in higher education institutions with provisions of the GDPR, where the experts evaluated the chances and threats of in the area of information and personal data management in higher education institutions being an outcome of the GDPR coming into force. The fifth chapter also includes the structure of

information security management, which was the achievement of the **project goal C3** of the present dissertation.

27 08 2018

Chmielaz