sciendo CzOTO 2019, volume 1, issue 1, pp. 226-233

SAFETY AT THE WORKPLACE – SELECTED ISSUES OF PERSONAL DATA SAFETY

doi: 10.2478/czoto-2019-0029
Date of submission of the article to the Editor: 18/11/2018
Date of acceptance of the article by the Editor: 29/12/2018

Grzegorz Chmielarz[1] – *orcid id: 0000-0002-1587-0733*
[1]Czestochowa University of Technology, **Poland,** *grzegorz.chmielarz@wz.pcz.pl*

Abstract: The paper presents the problem domain related to data safety management in the face of the threats that organisations of all types encounter in this scope. The Author's particular concern are personal data management issues, which are of key importance for contemporary enterprises as they frequently determine wining the market advantage and growth in their competitiveness. Yet, incidents of personal data breaches, aimed at economic organisations have been on the increase in the recent years, leading not only to substantial financial losses, but what is worse, frequently resulting in damage to their reputation. Therefore, a vital issue for all enterprises is to make their employees acquainted with threats to data security and their potential harmful effects on the operations and financial results of organisations. The paper presents an analysis of breaches to personal data in organisations in a global dimension as well as analyses of their negative effects to their image and trust of their customers.
Keywords: personal data, personal data safety, personal data management, threats to personal data

1. INTRODUCTION

As the Internet is a system that can be described as a collection of interconnected networks, everybody who can access one of these sub-networks by means of a computer and equipment that allows for free network connection is able to gain access to the whole of the information resources that are available on the Internet. Nowadays, such an access is not constrained by any time and space limitations, which makes it possible for both organisations and individual users to access and make available all types of information, frequently also the information of highly private nature. However, the easiness of accessing and sharing information resources on the Internet comes at a price, which is a growing number of threats that have appeared in the area of information safety management in recent years. Surely, not all types of information breaches breed the same consequences for organisations, yet cybercrimes that occur as a consequence of data breaches and the impact of these crimes on the economy in terms of damage and cost can be enormous. Frequently, such damages to individual organizations have been estimated in the hundreds of

millions of dollars. However, some costs are not easily measurable, such as impact on segments of the economy or national security (Algarni and Malaiya, 2016). Another issue is also a growing awareness of the Internet users on the amount of information, frequently of private nature, which they leave on the websites they visit. Contemporary consumers realise the fact that the digital trace they leave as a result of their activeness in the global network is registered and stored on the servers of Internet providers. This data about them is then used for marketing purposes and constitutes a measurable value for organisations that come into its possession. As currently personal data is being processed on a very large scale it is no wonder then that the users require a larger control over their personal data owned by organisations that manage and process it. These fears of Internet users are also reinforced by the ever-increasing number of breaches to personal data security. Statistics show that a growing number of attacks aimed at information resources of enterprises is being recorded and these figures have been growing year by year. In addition, according to the forecasts of experts the number of attacks directed at personal data of private individuals is going to increase in the years to come. So, it is of key importance for the organisations to take steps and attempt to develop proper behaviours of their employees in the area of data and information security management. Therefore, the underlying objective of the present paper is to analyse the main sources and types of breaches to personal data security in recent years. Based on secondary data that comes from specialist reports on personal data security, their impact, as well as literature on the subject the Author demonstrates potential negative consequences for organisations, in the financial as well as image dimension. Additionally, a particular stress of the paper is to analyse and focus on the role of so-called human error as a key factor that influences maintaining a proper level of personal data security in an organisation. It has also been the Author's intention to indicate the role of organisational culture and best practices in the scope of personal data security management as key factors that may significantly improve the security level of personal data processed in organisations. This information may constitute a valuable source of information for all organisations whose employees process personal data.

2. THREATS TO PERSONAL DATA SECURITY – DATA BREACHES ANALYSIS

Human preoccupation with the issue of providing security for personal data while working with computers, particularly in a networking environment, goes back as far as the 1960s of the previous century. In the late 1960s, scientists began worrying about the security implications of storing information on computers. Although discussed only in the context of classified information, the problems they recognized included confidentiality, integrity, and availability. The first widely published document The Ware Report, also known as Rand Report R-609, published by the RAND Corporation, identified computer security as an area of concern (Bishop, 2005). It was the first document that stressed the role of management and policy with reference to data safety computer security. It constituted a warning that utilisation of network solutions in information systems bred threats to their security. It is widely cited by computer security practitioners as framing the computer security field and is referred to in technical research articles on intrusion detection, high assurance, requirements engineering, and computer security education (Misa, 2016). In the 1980s of the past century, the decade when widespread computerisation affected almost all areas of life, cryptography was utilised as a major measure for protecting personal data

transmitted over high-speed electronic lines or stored in computer systems. There were two main concerns in this scope: preserving secrecy (or privacy), preventing an unauthorized disclosure of data and authenticity (or integrity), which consisted in preventing an unauthorized modification of data (Denning, 1982). The 1990s in turn witnessed a tremendous development of the Internet, which revolutionised the way people work with computers. The development of the new media resulted in two different attitudes to the notion of personal data security. Thus, differences were stressed between the needs of organisations whose main interest was still to protect all data using cryptographic mechanism and the ones that strived at a wider and more open use of the opportunities created by the global network. This required defining various policies of personal data management, which to a large extent were conditioned by the requirements in the scope of personal data security. The organisations that still adhered to purely cryptographic mechanisms focused on confidentiality of all its data. Their systems did not possess a network access as this could lead to data losses resulting from downloading information (deliberately or accidentally) residing on an unsecured remote system. indefinitely. For such organisations data integrity was important, but they would rather have their data deleted than read by unauthorized persons. On the other hand, there were organisations that still desired to maintain the integrity and confidentiality of their data resources, yet, they wanted their systems to be available via the Internet, which meant applying particular measures so as to make sure that the personal data in their possession would not become compromised (Bishop, 2003). Security concerns can also be blamed for hindrance of cloud computing services development in the first decade of the 21st century. Despite the fact that cloud computing was a fundamental change that occurred in the area of Information Technology and a representation of a movement towards the intensive and large scale specialization, yet, apart from convenience and efficiency problems it also brought challenges in the field of data security and privacy protection (Liu, 2015). This happened despite numerous potential advantages offered by the cloud computing model compared with the traditional IT models. However, currently, a shift can be observed in the area of personal data security with organisations' employees being considered an important element of information security systems, as it is their awareness as to the threats and sources of their origin, not the implemented IT protective measures, which frequently determines the security level of data and information in an organisation. Nowadays, the development of Information and Communication Technologies and increasing accessibility to the Internet have caused that organizations become vulnerable to various types of threats. There are still new ones appearing in this area, such as the recent threats related to a common application of the Internet of Things solutions. IoTs connected to the Internet have already become part of the social and economic infrastructure in everyday life of millions of people. The lives of users are becoming more efficient using IoTs and IoT services, which offer incredible power, still, their lives may suffer from more threats and breaches of privacy (Ando et al, 2016). Therefore, personal information ever more frequently becomes exposed to cyberattacks and their resulting damages, but distressingly often losses of personal information and data are caused by carelessness of the Internet users, including employees of various types of organisations. This seems to be confirmed by the latest statistics concerning reasons for personal data breaches. According to the report on data breaches in 2017 by Gemalto, the leading source of data breaches was

accidental loss which increased by 580% compared with the previous year reaching 2 billion of compromised records in 2017, although the number of incidents themselves was not the highest and amounted to 326 incidents. The next highest source of breaches was malicious outsider, which dropped by 44.6% from just over 1 billion records in 2016 to just over 585 million breached records in 2017. However, malicious outsider produced the greatest number of incidents – 1.269, which constitutes a 5% decline from 1.336 of such incidents that occurred in the previous year. The third highest source of data breaches in 2017 was malicious insider – 164 of such incidents against 179 in 2016, which is a decline by 8.4%, at the same time this type of a breach recorded a 117.3% increase in the number of compromised data records (from almost 14 thousand in 2016 to over 30 thousand in 2017). A small percentage of data breaches was caused by actions of hackers – 4 incidents or were sponsored by the country – just one incident. In the graphic form the data concerning primary reasons for data losses in 2017 has been presented in Figure 1.

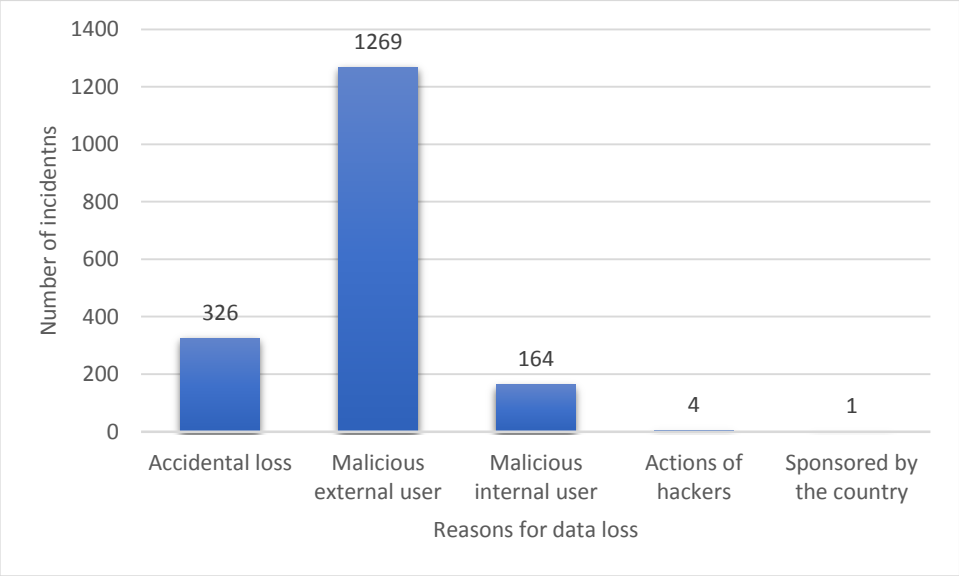

Fig. 1. Primary reasons for data losses in 2017

Source: own elaboration based on: *2017 The Year of Internal Threats and Accidental Data Breaches* – Report by Gemalto, available at: https://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf (access: 27.11.2018)

There have been many more examples of breaches to personal data security that have been brought to light, frequently resulting not only in substantial financial losses, but most importantly in a harm to reputation that can prove much more difficult to compensate for. According to the data provided by the Breach Level Index, more than 9 billion data records have been exposed in the years 2013-2018. However, in the first half of 2017 more than ten million records were compromised or exposed every day, while the information included in them ranged from medical, credit card to financial data or personally identifiable information. In the United States the ratio of the number of breaches to personal data security grew consequently in the years 2005-2017 reaching its peak in 2017. In this year almost 170 million of personal data records were revealed and the total number of personal data security breaches amounted to 1.579 billion. While comparing these figures with the year 2005 when

157 million of breaches to personal data occurred, one can notice that the growth was tremendous – over 1000% in 12 years. The sector most affected by breaches to personal data was the business sector, where 91.3% of all personal data disclosure occurrences took place. What is even worse only about 1% of the stolen, lost or compromised data used encryption, which made data retrieval impossible or much more time consuming for the thieves (https://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx). In the graphic form the data concerning breaches to personal data security in the USA in the years 2005-2017 has been presented in Figure 2.

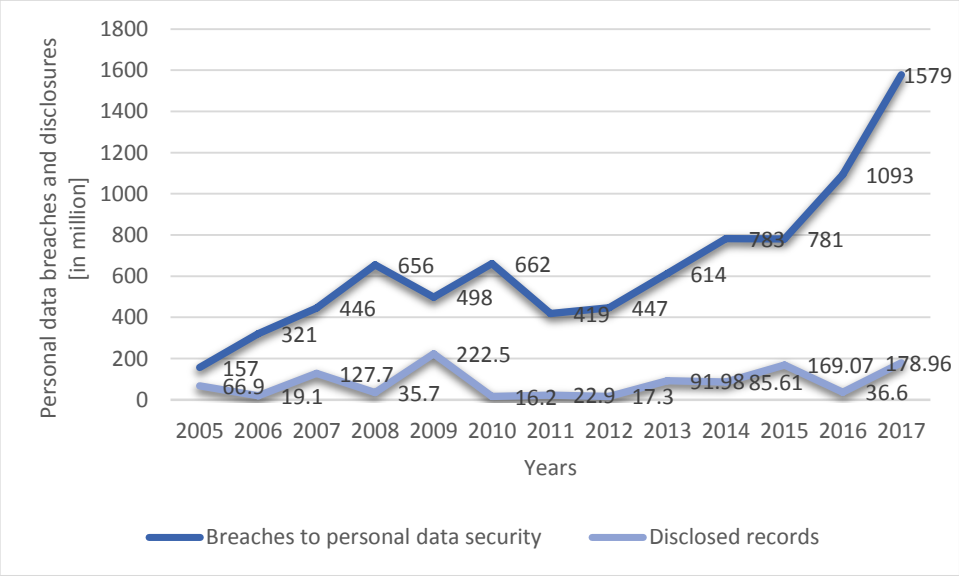

Fig. 2. Statistics on personal data breaches and disclosures in the United States in the years 2005 – 2017

Source: own elaboration based on: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (access: 27.11.2018)

It can be concluded then, that in recent years organisations have been constantly working on improving technological solutions that are supposed to ensure safety of possessed information resources and their efficiency in this scope has been growing. This also means that perpetrators who strive to obtain unauthorised access to information repositories of organisations have also changed their methods of attacks, which are presently aimed at employees of organisations who utilise in their professional duties IT products and services (Rocha et al, 2013).

3. HUMAN ERROR, ITS CONSEQUENCES FOR ORGANISATIONS AND MEASURES TO APPLY

Based on the statistics concerning data breaches presented in the previous chapter, it can be stated that the incidents of personal data being compromised have accompanied the development of the Internet, which itself has caused changes in the forms that work is being rendered in contemporary enterprises. One of them being application of mobile solutions, which has resulted in occurrences of new threats to information and personal data management security in organisations. Development of

mobile services created a possibility for employees to render work unconstrainedly form virtually any place in the world. As a growing number of organisations provide mobile equipment for their employees, they are able to work while travelling on business, can access their email accounts or company's applications just as if they were physically present in the company. However, mobile work and generally the fact of utilising by organisations computer networks to transfer information breeds particular problems in the scope of information and personal data protection. One of them is so called human error. It is said to be the main cause of an increase in data breaches despite an ongoing awareness of the necessity to implement appropriate education and processes to prevent such incidents. According to the data by Freedom of Information (FoI) one quarter of all data breaches between April and June 2014 involved the accidental loss or destruction of personal data caused by employees and around 43% of these were caused by sending data to the incorrect email or fax. In 2015 the Data Health Check report by Databarracks found that that humans were still the biggest security weak-link, and it advised firms that adopting a big business ethos can significantly reduce avoidable data losses (Jowitt, 2015). And the financial consequences for the companies that process large amounts of personal data cannot be underestimated. For example, in a personal data breach at eBay, which took place in 2014, information such as: surnames, addresses, dates of birth and passwords was stolen. It cost eBay over USD 200 million to repair the damages and pay the compensations, more importantly the company suffered also a significant damage to its reputation. Interestingly, the main reason of the breach was obtaining by hackers few passwords that belonged to the employees of eBay and this opened them access to the rest of the data. Another company, Heartland Payment Systems, due to a data breach lost over 130 million of data records, which resulted in significant losses for over 250 thousand of companies. Heartland Payment Systems had to pay giant compensations to organisations like Visa, MasterCard, American Express and others. In case of the next company, Target Stores, in 2013 its employees caused a leak of personal data where information about debit and credit cards of 40 million of the retail chain's customers. As a result, the company had to pay compensations that reached USD 170 million (https://www.cybercom.com/pl/Poland/security/security-blog-pl/ile-kosztuje-wyciek-danych--10-znanych-przypadkow). A more detailed summary of biggest breaches to personal data safety and their financial consequences for organisations has been presented in Table 1.

It needs to be stressed that breaches to personal data security are not limited only to large organisations. Small and medium-sized companies are equally prone to such occurrences. What is worse, a balance must be kept between protection of own resources and data about the customers and cooperation with service providers who make use of information possessed by these companies and can access all confidential data. Information about contractors, their bank accounts and addresses constitute sensitive information that needs to be highly protected as it can be subsequently used in personalised attacks aimed at these organisations. Two such occurrences took place in 2017. As a result of a cyberattack on Equifax in the USA personal data of almost 148 million of company's customers were compromised.

A human error was also the reason of another spectacular personal data breach in 2017 where over 1.3 billion of email addresses as well as physical addresses and surnames of customers of City Media were made public (https://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf).

Table 1
Biggest personal data breaches and their consequences for organisations

Affected company	Date of breach	Amount of stolen data	Financial losses
NASDAQ	2005-2012	160 mln	unknown
Heartland Payment Systems	2008-2009	130 mln	USD 110 mln
Sony Online Entertainment Services	2011	112 mln	USD 1.5 bn
Experian	2012	200 mln	unknown
American Database of Voters	2012	191 mln	unknown
Target Stores	2013	40 mln	USD 170 mln
eBay	2014	145 mln	USD 200 mln
The Home Depot	2014	56 mln	USD 80 mln
Epsilon	2015	60-250 mln	USD 4 bn
Anthem	2015	70-80 mln	over USD 100 mln

Source: (own elaboration based on: https://www.cybercom.com/pl/Poland/security/security-blog-pl/ile-kosztuje-wyciek-danych--10-znanych-przypadkow)

Thus, it seems that the problem of human error in the area of personal data security management needs to be addressed more seriously in organisations. One of the solutions involves creating a proper organisational culture, where interactions of employees within the information resources of an organisation actually contribute to its better protection. This means that a key process of information management in organisations is improvement in the culture of information protection so as to adjust behaviours of employees to requirements of information security and internal policies of information and personal data processing. There are three main factors distinguished that influence organisational culture in information and personal data protection area. The first of them is personnel training as personal data security constitutes an underlying responsibility of each employee. The trainings can take various forms and shall consider various aspects of organisation's operations. The second one concerns organising security procedures, where each of the employees is aware of potential threats to personal data security and knows how to react to various threats. The third one pertains application of new technologies and methods in the area of information security as each new measure decreases organisation's vulnerability to information loss (da Veiga and Martins, 2015).

4. CONCLUSION

Usefulness has become the most important role of IT technologies in managing contemporary organisations and information security management has become their primary focus. Currently, organisation's employees are thought to be a crucial element of information security systems, which often defines the security level of data and information in an organisation. The development of the Internet has caused that organisations have become vulnerable to various types of threats, one of them being breaches to personal data security. Accidental error and so-called human error are often to blame for incidents of personal data being compromised, which results in

substantial financial losses and a harm to reputation of organisations that process personal data records. The sector most affected by breaches to personal data is usually the business sector. Therefore, the issue of human error in the area of personal data security management is becoming more serious and requires implementation of additional security measures. One of them might be creating a proper organisational culture, in order to adjust behaviours of employees to the principles of information security as well as internal policies of information and personal data processing. The tools used for this purpose include personnel training for all employees, organising security procedures and implementing new technologies and methods so as to improve information security management in organisations.

REFERENCES

Algarni, A.M., Malaiya, Y.K., 2016. *A Consolidated Approach for Estimation of Data Security Breach Costs*. Proceedings of 2016 2nd International Conference on Information Management (ICIM2016), IEEE.

Ando, R., Shima, S., Takemura, T., 2016. *Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment.* IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, Volume E 99D, Issue 8, 1974-1981. DOI: 10.1587/transinf.2015INI0002

Bishop, M., 2003. *What is computer security*? IEEE Security and Privacy, Volume 1, Issue 1, 67-69. DOI: 10.1109/MSECP.2003.1176998

Bishop, M., Frincke, D.A., 2005. *Teaching secure programming.* IEEE Security and Privacy, Volume 3, Issue 5, 54-56.

da Veiga, A., Martins, N., 2015. *Improving the information security culture through monitoring and implementation actions illustrated through a case study*. Computers & Security 49, 162-176. DOI: 10.1016/j.cose.2014.12.006

Denning, D.A., 1982. *Cryptograpy and data security*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 3-4.

Jowit, T., *IT Security Spending To Reach £50bn, But Human Error Is Still Main Cause Of Data Loss*. http://www.silicon.co.uk

Liu, Y., 2015. *Privacy Protection Method in the Era of Cloud Computing and Big Data.* International Conference on Engineering Technology and Application (ICETA 2015), MATEC Web of Conferences, Volume 22, 1-4. DOI: 10.1051/matecconf/20152201041

Misa, T.J., *Computer Security Discourse at RAND, SDC, and NSA (1958-1970).* IEEE Annals of the History of Computing, Volume 38, Issue 4, 12-25. DOI: 10.1109/MAHC.2016.48

Rocha, F. W., Antonsen, E., Ekstedt, M., 2014. *Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture*. Computers&Security, Vol. 43, 90-110. DOI: 10.1016/j.cose.2014.03.004

https://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx

https://www.cybercom.com/pl/Poland/security/security-blog-pl/ile-kosztuje-wyciek-danych--10-znanych-przypadkow

https://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf