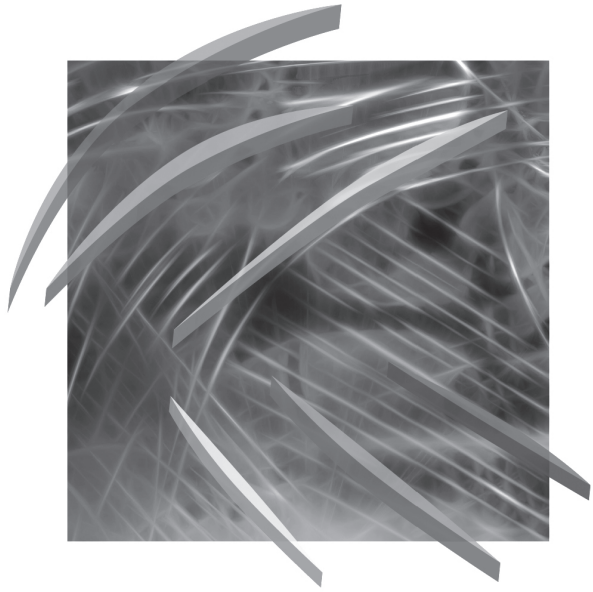
INFORMATYKA EKONOMICZNA

BUSINESS INFORMATICS

1(39)•2016



Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu
Wrocław 2016

Redakcja wydawnicza: Elżbieta Macauley, Joanna Świrska-Korłub
Redakcja techniczna: Barbara Łopusiewicz
Korekta: Barbara Cibis
Łamanie: Małgorzata Myszkowska
Projekt okładki: Beata Dębska

Informacje o naborze artykułów i zasadach recenzowania
znajdują się na stronach internetowych
www.wydawnictwo.ue.wroc.pl
www.businessinformatics.ue.wroc.pl

ISSN 1507-3858
e-ISSN 2450-0003

Wersja pierwotna: publikacja drukowana

Zamówienia na opublikowane prace należy składać na adres:
Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu
ul. Komandorska 118/120, 53-345 Wrocław
tel./fax 71 36 80 602; e-mail:econbook@ue.wroc.pl
www.ksiegarnia.ue.wroc.pl

Druk i oprawa: TOTEM

Spis treści

Wstęp

Drodzy Autorzy i Czytelnicy, po raz kolejny mamy przyjemność złożyć na Wasze ręce opracowanie z serii „Informatyka Ekonomiczna".

W przedkładanym numerze znalazły się teksty Autorów będących przedstawicielami różnych ośrodków naukowo-badawczych z Polski, a także opracowania powstałe w ścisłej współpracy z doświadczonymi praktykami gospodarczymi. Niezmiernie wartościową cechą opracowań wydanych w czasopiśmie „Informatyka Ekonomiczna" jest to, że stanowią one prezentację różnorodnych punktów widzenia i poglądów dotyczących zastosowania nowoczesnych rozwiązań z obszaru ICT. Perspektywy i opinie prezentowane przez Autorów tekstów niejednokrotnie pozwalają Czytelnikom na poszerzenie przemyśleń dotyczących ich poglądu na temat możliwości i kierunków zastosowania technologii informacyjno-komunikacyjnych w praktyce gospodarczej.

Nie wszystkie artykuły nadesłane do naszego czasopisma spełniają jednak jego wymogi formalno-merytoryczne, co zwiększa znaczenie i wartość publikacji, które otrzymały podwójne pozytywne recenzje i zostały wybrane do opublikowania w aktualnym numerze „Informatyki Ekonomicznej".

Redaktor niniejszego wydania pragnie wyrazić podziękowania wszystkim Autorom, którzy zechcieli podzielić się swoimi doświadczeniami i poglądami. Ponadto składa podziękowanie Recenzentom za wnikliwe i rzeczowe oceny przedkładanych tekstów.

Iwona Chomiak-Orsa

INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 1(39) • 2016

ISSN 1507-3858
e-ISSN 2450-0003

Michał Dziadkiewicz, Nicoletta Baskiewicz
Politechnika Częstochowska
e-mails: michaldziadkiewicz@gmail.com; nicoletta-p@o2.pl

MANAGING THE PROCESS OF ELECTRONIC COMMUNICATION IN A SMALL LEGAL FIRM

ZARZĄDZANIE PROCESEM KOMUNIKACJI ELEKTRONICZNEJ W MAŁEJ KANCELARII PRAWNEJ

DOI: 10.15611/ie.2016.1.06
JEL Classification: M150, K190

Summary: The purpose of this article is to present the issues related to the management process in the electronic communication of a small law firm. In the introduction, the role of information and knowledge in shaping the competitiveness of enterprises is presented. Then the phenomenon of electronic communication as a process of data transmission is shown, which on the one hand determines the competitive position of economic entities including law firms and legal counsellors, and on the other hand, it is the subject of legal regulations. Because the information provided by electronic means shall be subject to the professional secrecy of legal attorneys or solicitors, as the principle of confidentiality applicable to lawyers according to relevant legislation does not exempt these entities from the responsibility in terms of the protection of personal data. Another area raised in the article is to identify actions to protect information transmitted electronically. The last part of the study is to present the results of studies that show the extent to which we use e-mail, free applications such as Dropbox and Google Drive. Moreover the issues of the frequency of password changing and encryption of media as well as attacks on data owned by an office have been discussed. The whole content has been summarized with conclusions.

Keywords: electronic communication process, electronic document, legal regulations on personal data protection, legal professional privilege.

Streszczenie: Celem niniejszego artykułu jest prezentacja problematyki związanej z zarządzaniem procesem komunikacji elektronicznej w małej kancelarii prawnej. Na wstępie przestawiono rolę informacji i wiedzy w kształtowaniu konkurencyjności przedsiębiorstw. Następnie ukazano zjawisko komunikacji elektronicznej jako procesu przesyłu danych, z jednej strony determinujące pozycję konkurencyjną przedmiotów gospodarczych, w tym kancelarii prawnych i radcowskich, a z drugiej stanowiące podmiot regulacji prawnych. Informacje przekazywane również drogą elektroniczną podlegają bowiem tajemnicy zawodowej osób wykonujących zawód adwokata czy radcy prawnego, gdyż zasady zachowania tajemnicy

obowiązującej adwokatów i radców prawnych z mocy właściwych ustaw nie zwalniają tych podmiotów ze stosowania w zakresie ochrony danych osobowych. Kolejnym zagadnieniem poruszonym w artykule jest identyfikacja działań ukierunkowanych na ochronę informacji przekazywanych drogą elektroniczną. Ostatnim elementem opracowania jest prezentacja wyników badań wskazujących, w jakim zakresie używa się poczty elektronicznej, bezpłatnych aplikacji typu Dropbox, Google Drive. Dodatkowo w tekście poruszono kwestie częstotliwości zmiany hasła, szyfrowania nośników danych oraz ataków na dane kancelarii.

Słowa kluczowe: proces komunikacji elektronicznej, dokument elektroniczny, regulacje prawne dotyczące ochrony danych osobowych, tajemnica adwokacka.

1. Introduction

In contemporary management theory, with particular consideration of the resources concept [Brown, Davidsson, Wiklund 2001; Krupski 2009] an increasingly popular subject is the nature of information [Tiwana 2002] which, next to knowledge, is treated as a key resource [Senge 2002], allowing to gain strategic advantage [Grant 1996]. Information fits into the invisible resources of the company, as part of these resources the ones, in respect of which the company is entitled as an owner, are specified − patents, licenses, contacts, trade secrets and database [Godziszewski 2001]. This information is acquired and stored by a company mostly in the form of electronic documents.

As part of the statutory definitions, an electronic document is regarded as an individual semantic set of data arranged in a specific internal structure and stored on a computer data carrier [Ustawa z dnia 17 lutego 2005 r.…], or even for the purpose of criminal proceedings any written medium of information, regardless of the fact that this media is a document within the meaning of civil, or administrative law [Stefański (ed.) 2015]. An entrepreneur − lawyer, legal adviser − uses electronic communication including email, phone communication and the so-called cloud data to a large extent. It should therefore implement the principle of the management of this information to ensure the achievement of its minimum targets:

– document security meeting the requirements of legal privilege of a legal advisor or attorney,
– processing of such data in such a way that the office personnel has the opportunity to use and develop its intellectual capital (developed process solutions, patterns of letters, contracts, opinions, etc.).

The electronic document has a content of data like text, image, sound, logical structure with the presence of metadata − information identifying date, parameters, or information about the type of data represented [Jankowski 2009].

2. Electronic communication as a matter of statutory regulations with regard to law firms

The importance of information used in the process of the functioning of law firms should be considered in two planes. The first is common to all companies as an issue of the competitive struggle, which is becoming increasingly significant due to the continued growth in the number of providers of legal services, while the other plane are the legal regulations, including those that apply only to legal services and those which should be observed by the actors under the generally applicable law.

This first group of regulations is a system of rules relating to the obligation of the professional secrecy of a lawyer, the other is the rules governing the authorities' access to information held by certain entities, as well as provisions on the duty to protect the information by the accumulating entities. The topic is illustrated by the law on the access to state services information in the so-called operational control commonly known as the "Act on Surveillance", as well as having a very widely influential law on the protection of personal data. The term "Act on Surveillance" covers the Act of 15th January 2016 which amends the Act on Police and other acts.

The confrontation of the statutory term of operational control with regulations governing the activities of law firms or legal advisers indicates the possibility of the penetration of bodies authorized to use operational control in the sphere covered by professional secrecy. The obligation of professional secrecy of a lawyer is standardized in article 6 of the Act of 26 May 1982, Law on the Bar, and the corresponding obligation relating to legal advisers − in art. 3 it.3-6 of the Act of 6 July 1982. According to these regulations, the professional secrecy of a lawyer or solicitor is all about what he/she learned in connection with the provision of legal aid or conducting cases. The obligation of professional secrecy is unlimited in time and no lawyer may be released of it as to the facts which he/she learned while providing legal aid or conducting a case.

The obligation to maintain secrecy does not include the information provided on the basis of the provisions of the Act of 16 November 2000 on counteracting money laundering and financing terrorism (Off. Jour. of 2014. it. 455) − within the meaning specified by those regulations.

The scope of information constituting the professional secrets of a lawyer, being subject to the provisions of the Bar Act and the information security measures are also referred to in paragraph 19 of the Compendium of Rules on Advocates' Ethics and the Dignity of the Profession (Advocates' Code of Ethics). The very same provision clarifies the fact that the lawyer is obliged to keep secret everything he/she learned in connection with the performance of his/her professional duties, in addition to professional secrecy covering all material contained in the legal files, as well as all the news, notes and documents relating to the case obtained from the client and others, regardless their location.

In relation to solicitors, a similar clarification is contained in the provisions of paragraphs 12-18 of the Solicitors' Code of Ethics.

2.1. Professional secrecy

On the basis of the provisions referred to and the codes of professional ethics of advocates and legal advisers (solicitors), one can formulate general conclusions as to the ways and means to protect information covered by the professional secrecy of advocates or solicitors, which can be called law firm's secrets in a simplified form.

The regulations in the field of information covered by legal privilege or secrecy distinguish between the projects of an organizational and a technical nature.

The former includes a commitment by the lawyer of all his/her colleagues and staff, including those employed by the him/her in the process of professional activity, to observe professional secrecy, the latter, however, in the case of using a computer or other means of electronically recorded data − is the obligation to apply safe software and other data protection measures against unauthorized disclosure. It is implied thus, that these measures should present the highest possible standard and be the most effective. The Solicitors' Code of Ethics does not say directly anything about the actual use of electronic devices as carriers of information, however a similar obligation to use the information security measures provides the obligation to protect them in the best possible way

In cases of the transfer of information covered by professional secrecy by means of electronic or similar media, an advocate is required to act with special care and warn the customer about the risks of confidentiality related to the means of communication or correspondence. A similar obligation applies to solicitors.

Going back to the abovementioned "Act on Surveillance" and the possibility of obtaining access to information covered by legal privilege of authorized services, it should be noted that these opportunities arise directly from the Act, and the implementation of operational control and using the measures provided for by law, remains outside an advocate's or solicitor's influence. Nevertheless, the "Act on Surveillance" does not prohibit taking up by the law firms all the available means of protection of data and information captured on electronic media, or transmitted via electronic mail.

In order to maintain the highest possible level of security of data and information, it is advisable to use a variety of security measures ranging from the selection of information by extracting such that may be in no case discussed through telephone calls, e-mails (e-mails) or letters sent by traditional mail. Such information should only be discussed in direct talks with the client, and any notes made on the traditional paper media should be especially protected and destroyed mechanically at the moment when they are no longer needed. Archiving such information and data or their transfer onto electronic media should be excluded.

If it is necessary to conduct correspondence with the technical means and the use of telecommunications networks, which can be inevitable, one should particularly

think about the content of the correspondence, and e-mails should have protection with the highest performance possible. One should avoid e-mailing documents, photos or files held or produced in connection with the activities of the office, thus preventing them from being intercepted by the wrong hands, for example by leaving them on the computer of the recipient (client). When using e-mail one should adopt the principle of an effective clearing of used correspondence.

2.2. Personal data protection

Another problem posed in the course of deliberations on the safety of electronic communication is the issue of the adequate protection of personal data owned and processed by the law firm in its operations. The relationship between data protection is obvious for provisions on the protection of personal data and also applies to the information that clients of the law firms entrust to advocates or solicitors assuming their confidentiality.

The basic legal act in the field of personal data protection is the Act of 29 August 1997. On personal data protection (Off. Jour. 2014. Item. 1182, as amended D.). The Act comprehensively regulates the issue of protection of personal data, both in the personal and objective aspects.

Among the entities obliged to implement the provisions of the Law on Personal Data Protection are law firms. This follows from the content of article 3, para. 2, Section 2 of the Act, which states that the Act also applies to natural persons and legal persons and organizational units without legal personality, if the processing of personal data is related to the professional activity or for the implementation of statutory objectives and if these firms are established or resident on Polish territory, or in a third country, unless the processing of personal data by means of technical devices is located on Polish territory.

From an objective point of view − the regulations of the Law on Protection of Personal Data refer to any information relating to an identified or identifiable natural person. An identifiable person is one which can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social features.

To summarize − the principle of confidentiality applicable to advocates and solicitors under the relevant laws do not exempt these entities from the application of the data protection provisions of the Act on the Protection of Personal Data. The consequence of this situation is to require law firms to observe the duties under this Act, except for the application for registration of datasets of clients or individuals who concluded contracts for the provision of legal services to the Chief Inspector for Personal Data Protection (art. 43 paragraph 1, point 5 of the Act on the Protection of Personal Data). It should be noted, however, that the obligation to register personal data occurs if the firm will create a collection for purposes not related to the provision of legal services.

As practice shows, the law firms carry out the processing of personal data within the meaning of art. 7, point 2 of the Act on the Protection of Personal Data. Under this provision, any operation performed upon personal data such as collection, recording, storage, organization, alteration, disclosure and erasure and especially those operations performed in the computer systems, are defined as processing. Law firms are therefore included in the group of data controllers, according to art. 3 paragraphs 2 point 2, and art. 7 Section 4 of the Act on the Protection of Personal Data.

The basic duties of law firms in the field of protection of personal data is to obtain the consent of the data, subject to the continued processing of those data, except for their removal and subsequent observance of all obligations of data administrator defined in the provisions of Chapter 3 of the Act on the Protection of Personal Data (Art. 23-31a of the Act). The consent of the legal client entrusting one's personal data should be reflected in the contract for the provision of the legal services concluded between the firm and the client.

Another duty of a legal firm as the data controller, is to use the appropriate technical and organizational measures ensuring the protection of personal data being processed, accordingly to the risks and category of data being protected, and in particular according to the obligation to protect data against their unauthorized disclosure, takeover by an unauthorized person, processing with violation of the Act, change, loss, damage or destruction (art. 36, paragraph 1 of the Act on the Protection of Personal Data). Furthermore, data controllers are required to keep records describing the processing of personal data and the applied security measures (art. 36, paragraph 2 of the Act on the Protection of Personal Data).

The basic measures for the protection of personal data processed in information systems which should be used in a legal firm include:

1) to adjust the level of security of information systems used to the treatment of personal data,
2) the use of advanced safety systems of data processed in IT systems and detect intrusion attempts to office systems,
3) the use of electronic mail services with appropriate security of transmitted data, preferably through the use of encryption systems.

In general, the protection of personal data (and other information which constitutes a trade secret of a legal firm) in the information system should provide:

1) confidentiality by preventing third parties' access to the data,
2) information integrity by preventing unauthorized changes to the data,
3) the availability of information on each request of the entitled person,
4) control of access to information by creating and storing the history of access to the data with information about the persons who obtained this access.

In addition to the above, in both cases, data processing using electronic devices, as well as for traditional forms of data collection and processing, one should pay attention to the proper protection of the office space and storage of one's documents,

against the free and uncontrolled access of third parties. It is also effective to perform destruction and removal of any unnecessary documents collected in connection with the cases.

In addition to security measures of a technical nature, it is necessary to undertake organizational activities. Whatever the organizational form in which the law firm operates is, it is required to hold a document concerning the protection of personal data in the form of a Security Policy for Personal Data and Information Systems Management Guidelines. In such documentation, among others, one needs to extract personal data files.

The basic organizational activities include:

1) training of all office employees in the fundamental issues of data protection and application of security measures,

2) the execution of requirements of all office workers' obligations concerning confidentiality in relation to personal data and ways to protect them,

3) adopting the principle of differentiation in the rights of employees in the firm, concerning the necessary basic level as one for the allocation of the minimum powers necessary to perform the entrusted work.

In the practice of law firms, each of these methods should be developed and modified according to the needs, particularly when referred to the scope and type of data collected and processed.

3. Electronic communications and data security in a small legal firm − an empirical study

As part of this paper, in May 2016 a survey among advocates and solicitors was carried out which engaged the so-called sole law entrepreneurs in the city of Czestochowa. These are the entities where the owner is a lawyer employing no more than a few employees and having a similar group of collaborators (persons involved in the preparation of documents reviews, attending hearings, etc.). Fifty questionnaires were sent by electronic means and in hard copies, of which 34 were successfully completed and the survey included a complementary uncategorized test method focused on broadening knowledge about attacks on information recorded on electronic data carriers.

Figure 1 illustrates the scope of the use of e-mail in the work of law firms. E-mail is widely used as means of communication, where the majority of companies (94%) uses this channel to transmit pleadings, opinions, contracts and therefore electronic documents that may contain information covered by legal privilege.

A smaller percentage of subjects − 53% − uses the so-called clouds. In the assessment of managers, the barriers which have the strongest impact on uses of cloud often are: legal jurisdiction, security and data protection, trust, data access and portability, data location, local support, change control, ownership and customization, evaluation of usefulness, slow internet connection, local language and tax incentives.

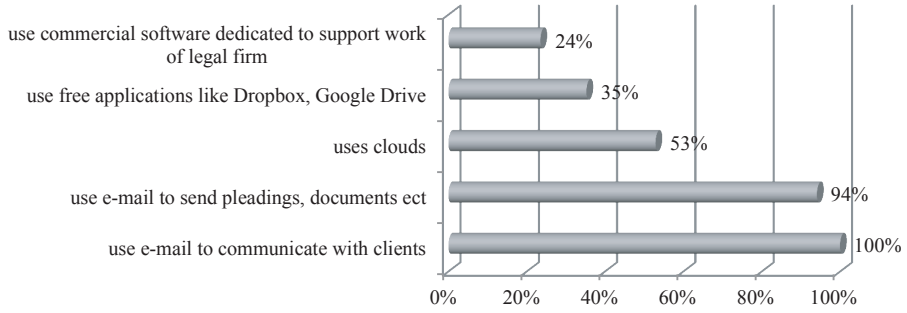


Figure 1. The scope of the use of e-mail in the work of Law Firm

Source: own study based on research results.

As it was shown in the cited report, none of the barriers can be accepted as the only most important one which was mentioned by most of the respondents [Jelonek et al. 2014]. This technology is used in the exchange of knowledge between employees to cooperate in the conduct of individual cases, transmission of photographs, documents in the case, 35% of subjects uses free applications like Google Drive or Dropbox. Only 24% of subjects decided to purchase commercial software to manage office calendar, electronic case of files, etc.

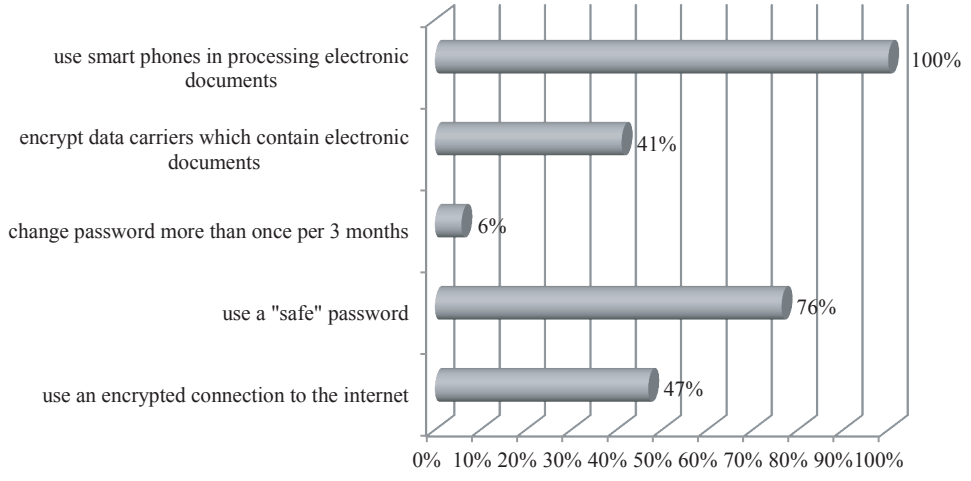


Figure 2. The approach to security of transfer and storage of electronic documents

Source: own study based on research results.

Given the prevalence of the use of e-mails to communicate with clients , we must be concerned by the approach to security of the transfer and storage of electronic

documents presented by the surveyed entities as illustrated in Figure 2. Only 41% of respondents encrypt media data which are stored in electronic documents and worth highlighting is the fact that they are often stored on a laptop computer which is transported from the office to the clients' premises and then home. What is more, only 47% of entities send their electronic documents from an encrypted Internet connection, even worse as many as 76% of entities use the so-called secure password to access the data. The secure password in this paper is understood as a password that is at least eight characters long, does not contain one's user name, real name, or company name, does not contain whole words, contains other characters than letters and differs significantly from previous passwords. However, only 6% of the surveyed entities changed their password more than once every three months.

The weakest link in the security of the stored data should be considered smartphones, which were used by 100% of the subjects, the devices were used for recording court records or include logging into e-mail or free cloud.

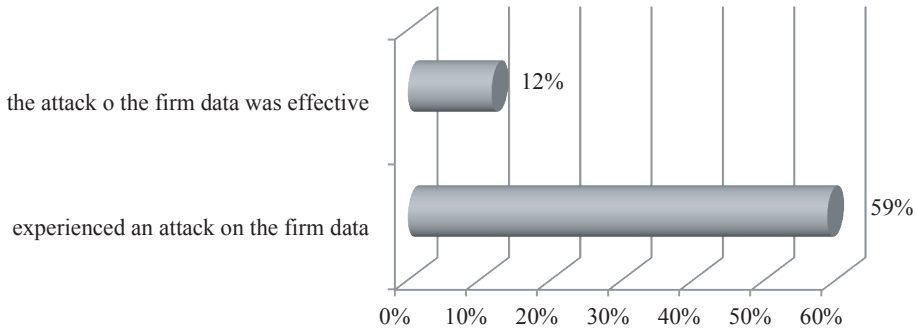


Figure 3. The frequency of attacks on data of law firms

Source: own study based on research results.

Figure 3 illustrated the issues of the attack on the office data which happened to 59% of the companies surveyed. Attempts to attack consisted of sending an e-mail, the opening of which resulted in encrypting files on the disk, possibly with an attempt to extort data credentials. It should be noted that 12% of the attacks were effective. Based on the results of a survey conducted, it was possible to obtain detailed information in this regard, showing that effective attacks were carried out by sending an e -mail pretending to be sent by the Polish Post Office, after opening the attachment malware encrypted files on one's computer, demanding a "ransom" for password access. The surveyed subjects have never been subject to an attack consisting in copying the data and the threat of spreading them in the web.

4. Conclusion

The aim of this paper was to present the issue of threats to electronic and personal data, and the effective methods to protect data against the abovementioned threats and unauthorized access. Both business practice and literature in the field of electronic communication process management stress the need to care for the information transmitted electronically. Given the characteristics of the work of both advocates and solicitors, this problem seems to be extremely important considering the scope and nature of the transmitted information most frequently covered by professional secrecy. This secrecy and the necessity of confidentiality results both from the legislation and the codes of ethics adopted by professional associations.

The study indicates the need to implement smart policies aimed at protecting data and this is due to the significant threat of attacks conducted via e-mail, which happened to 59% of the subjects and also due to the negative impact of the legal environment. This will maintain the image of the profession among clients as to guarantee their rights, an important factor of which is the actual protection of data entrusted by clients. According to the authors, the importance of data protection will increase with time as will the techniques used by cyber-criminals operating in the web.

References

Brown T.E., Davidsson P., Wiklund J., 2001, *An operationalization of stevenson's conceptualization of entrepreneurship as opportunity-based firm behaviour*, Strategic Management Journal, vol. 22.

Godziszewski B., 2001, *Zasobowe uwarunkowania strategii przedsiębiorstwa*, Wydawnictwo Uniwersytetu Mikołaja Kopernika, Toruń.

Grant R., 1996, *Prospering in a dynamically-competitive environments: Organizational capability as knowledge integration*, Organization Science, vol. 7, no. 4, p. 380.

Jankowski J., 2009, *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji*, Difin, Warszawa.

Jelonek D., Stępniak C., Turek T., Ziora L., 2014, *Identification of mental barriers in the implementation of Cloud Computing in the SMEs in Poland*, Annals of Computer Science and Information Systems, vol. 2, Warsaw.

Krupski R., 2009, *O szkole zasobów zarządzania strategicznego inaczej*, Przegląd Organizacji, nr 3.

Senge P.M., 2002, *Piąta dyscyplina. Teoria i praktyka organizacji uczącej się*, Oficyna Ekonomiczna, Kraków.

Stefański A. (red.), 2015, *Kodeks karny. Komentarz*, wyd. 2, Legalis, Warszawa.

Tiwana A., 2002, *The Knowledge Management Toolkit. The Knowledge Management Toolkit. Orchestrating IT, Strategy, and Knowledge Platforms*, Prentice Hall PTR, Upper Saddle River, New York.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.