INFORMATION
SYSTEMS IN
MANAGEMENT

Information Systems in Management (2016) Vol. 5 (1) 66−77

INFORMATION SECURITY MANAGEMENT SYSTEMS IN MUNICIPAL OFFICES IN POLAND

DOMINIKA LISIAK-FELICKA [a)], MACIEJ SZMIT [b)]

[a)] *Department of Computer Science in Economics, Faculty of Economics and Sociology, University of Lodz*
[b)] *Orange Labs Poland*

The article presents results of a survey concerning Information Security Management Systems (ISMS), which was conducted in municipal offices between December 2014 and June 2015. The aim of the research was identifying in which municipal offices information security management systems are implemented, according to which standards ISMS are developed and certified and gathering information about: factors facilitate the implementation, problems encountered in the implementation process and offices' documentation concerning information security.

Keywords: information security, information security management systems, information security policy

1. Introduction

Information Security Management System (ISMS) is defined in ISO/IEC 27000 standard as part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. This system is applicable for all types of organizations, also for public administration units [1, 2].

The regulation of Polish Council of Ministers regarding to the National Interoperability Framework, containing minimum requirements for public registry and information exchange in electronic form and the minimum requirements for

ICT systems [11] imposing on managers of public administration units some obligations relating to security management, such as following:

- establish, implement, operate, monitor, review, maintain and improve information security management system,
- provide an update of internal regulations,
- maintenance hardware and software inventory, which are used in information processing,
- conduct periodic risk analyzes,
- permissions management,
- provide training on information security,
- protect of processed information,
- ensure an adequate level of security in ICT systems,
- immediately report information security incidents in a defined and fixed way for taking quick corrective action,
- provide periodic internal audit of information security.

The numbers of information security incidents have grown rapidly. This is confirmed by the Governmental Computer Security Incident Response Team (CERT.GOV.PL) reports. According to the "Report on the cybersecurity state of Poland" in 2014 [12] CERT.GOV.PL registered 12017 notifications, which 7498 were classified as incidents. For comparison, in 2013 [13] there were 8817 notifications and 5670 information security incidents.

There are many information security incidents in public administration in Poland. The latest incidents in municipal offices, which were commented, were e.g.:

- on the website of city office in Poznan, the information for logging into training and test versions of System Support Authorities Election were available [17];
- personal information leaked from the city office in Piotrków Trybunalski. The district prosecutor's office launched an investigation into the illegal sharing of personal data by the municipality initiators of the referendum [18];
- attack on the website of the city office in Torun. The website was swapped. The administrators had to quickly restore the original website [19, 20];
- cybercriminals stole a total of 2.1 million PLN from five municipal offices (Belsk Duży, Błażowa, Gidle, Rząśnia, Jaworzno). They broke into computer systems and using malware changed account numbers outgoing transfers from the municipal office [21, 22, 23, 24].

2. Aim and method of the research

The survey is a part of our investigations concerning selected aspects of cybersecurity in public administration in Poland [3, 4, 5, 6, 7].

The aim of research was identifying in which municipal offices information security management systems are implemented, according to which standards are developed and certified, the reasons why respondents did decide (or not) to implement and certification of ISMS and collect information about:

- factors that facilitate the implementation of the information security management system,
- problems with the implementation of the system,
- operations relating to the functioning of the system, which officials have the most problems,
- information security training in offices,
- reviews of information security policy,
- information security incident management,
- documentation relating to information security.

The research was conducted using a survey questionnaire. Email letters with asking to participate in the survey to 800 randomly selected municipal offices in Poland were sent (stratified random sampling was used). Obtained 146 positive responses including: 40 urban municipalities, 43 urban-rural municipalities and 63 rural municipalities [16].

3. Results of the research

Among the 146 municipal offices, only in 51 the information security management system is implemented. In the 95 offices such a system does not work and in the past only 5 offices had attempted to implement it (see Figure 1).

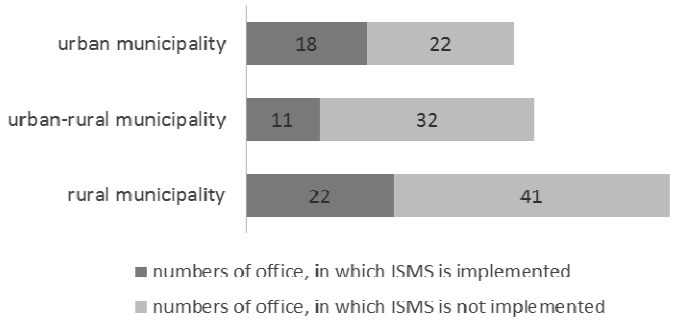

Figure 1. Information Security Management Systems in municipal offices

The reasons, why the officials did not implement ISMS, include: lack of funds (71 indications), lack of sufficient knowledge (31 indications) and lack of time (30 indications).

Seventeen of the 51 implemented Information Security Management Systems were developed by the recommendations of the standards: five offices were using ISO/IEC 27002, four offices were using PN-ISO/IEC 17799, and two offices using BS-07799-1. Officials also indicated the following standards (one indication for each standard): PN-I-07799-2, PN-EN ISO 9001 (this standard is not associated with information security), ISO/IEC 27001, PN-ISO/IEC 27001. Two officials did not specify any standards.

Only three offices decided to certify the information security management system according to PN-ISO/IEC 27001.

In offices which not decided to certify their ISMS, the following reasons for not taking such action were indicated:

- it is an expensive proposition (14 answers),
- certification does not affect the quality of the information security management (5 answers),
- it is a time-consuming project (4 answers),
- it is unnecessary (2 answers).

Another question examined the ISMS implementation time. Answers to this question are shown in Figure 2.

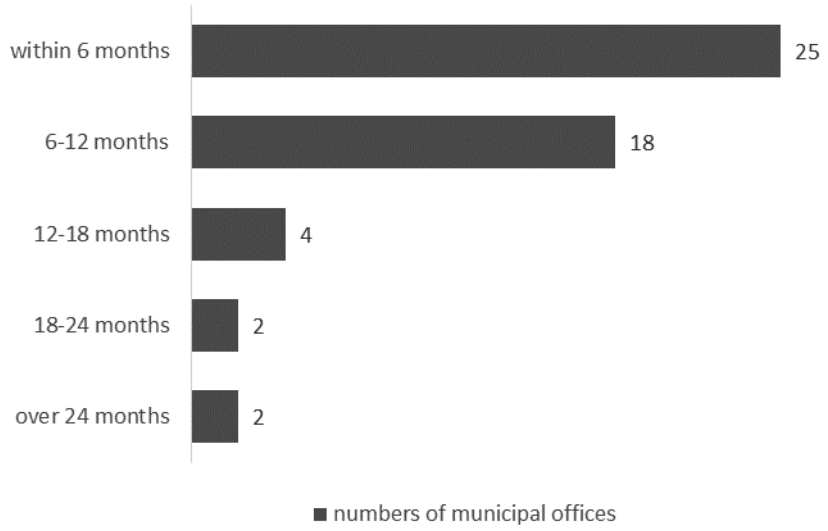

Figure 2. ISMS implementation time in the surveyed municipal offices

Next figure (Figure 3) presents the ISMS implementation success factors. The most important are: allocation of adequate financial resources, substantive preparation of employees, involvement of the top management, employees awareness of the need to ensure the security of information.

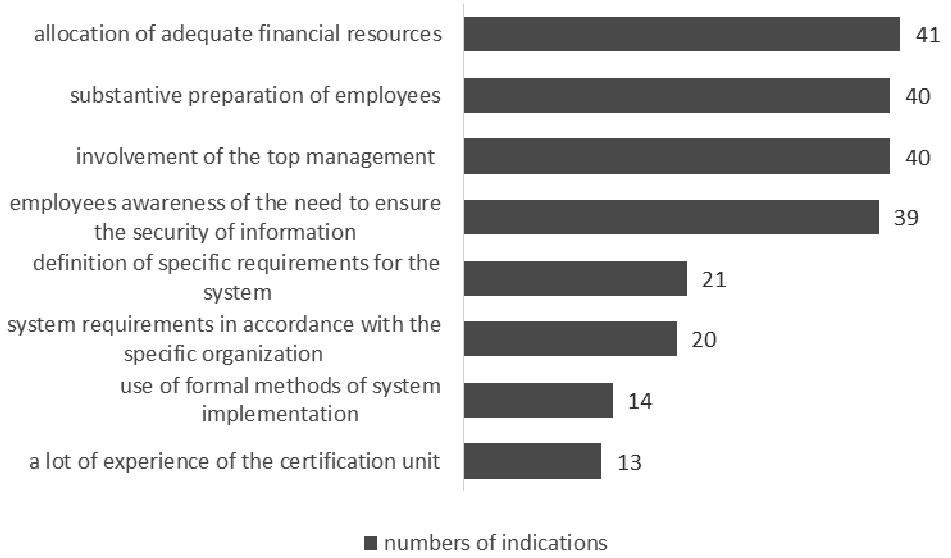

Figure 3. Evaluation of factors that facilitate the implementation of the ISMS

Another success factors indicated by officials are: IT support, employment of IT staff in the number of people appropriate to the size of the organization and implementation of other certified systems, for example, quality management system ISO 9001.

Officials were asked to indicate problems with the implementation of the ISMS. Respondents indicated as the sources of problems:

- too extensive documentation (35 answers),
- insufficient financial resources (23 answers),
- lack of substantive preparation of employees (21 answers),
- lack of use of formal methods of implementation of the system (16 answers),
- lack of involvement of top management unit (13 answers),
- lack of experience of certification unit (3 answers).

Another problems indicated by officials are: lack of human resources, large workload and opposition of IT staff.

According to officials, the implementation of Information Security Management System has a positive effect on the unit, especially raises awareness of information security management among employees. It is a time-consuming but can increase the level the information security, is necessary and beneficial. The 18 officials also indicated that it is an expensive venture (Figure 4).

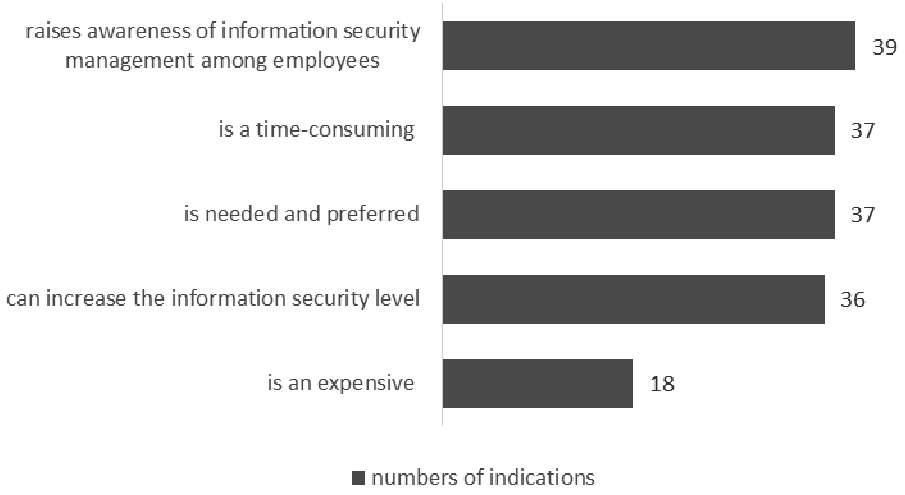

Figure 4. Opinion on the ISMS implementation

Respondents also indicated the steps on the operation of the Information Security Management System, which have the most problems. The most indications received the following:

- performance of procedures for monitoring and reviewing the safety information,
- conduct internal audits of the system,
- preparation of relevant documentation,
- cooperation with the users of the system.

The results are shown in Figure 5.

Officials also indicated problems with an excessive load of other tasks not related to information security and a current supervision of compliance with procedures by users.

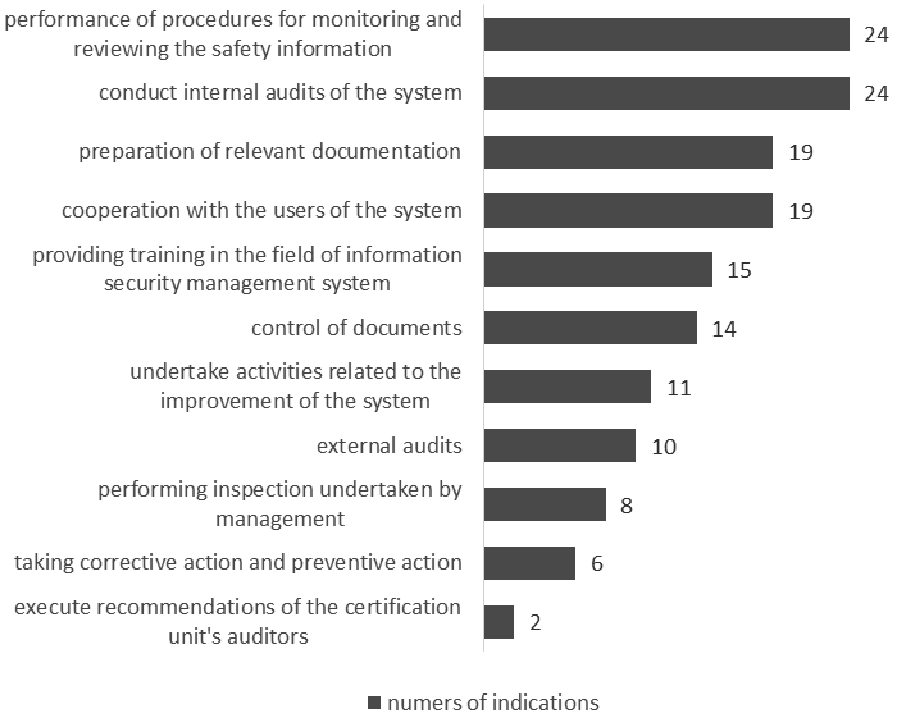

Figure 5. Actions on the operation of the ISMS, which officials have the most problems

Only 10 offices of the 51 implementing an Information Security Management System were able to count on the support of the state administration bodies.
The stages in which the aid was granted:

- the establishment information security management system (5 answers),
- implementation and operation of information security management system (5 answer),
- monitoring and review of information security management system (1 answers),
- maintaining and improving information security management system (2 answer).

Unfortunately, none of the officials present the information about received support.
Another survey questions focused on conducting documentation. Among the 146 surveyed offices, 113 have developed and implemented an information security policy that contains the policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data [8, 10, 14, 15], and 28

offices have only a policy of protection of personal data in accordance with the requirements of this Law. Five units do not have appropriate documentation. Table 1 presents the characteristics of each document.

Table 1. Characteristics of information security documentation in municipal offices (U –urban municipality, U-R – urban-rural municipality, R – rural municipality)

Types of document	U	U-R	R	Total
an information security policy that contains the policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data	31	35	47	113
policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data	7	8	13	28
none	2	0	3	5
Summary:	**40**	**43**	**63**	**146**

It needs to be highlighted that:

- in 15 municipal offices Information Security Administrators have not been appointed;
- in 20 units trainings of implemented information security policies have not been conducted;
- in 34 municipal offices trainings in information security, information systems security, data protection had not been conducted.

Among the 146 units in 141 the security reviews are conducted. The frequency of these inspections is shown in Figure 6.

Security policy reviews can be conducted every few months, or when necessary, but it is neither possible nor purposeful to review the policies every day or even every week (information security documentation in surveyed offices have at least several dozen pages). Such answers mean that the respondents did not understand the issue contained in the question, or at least they made a mistake.

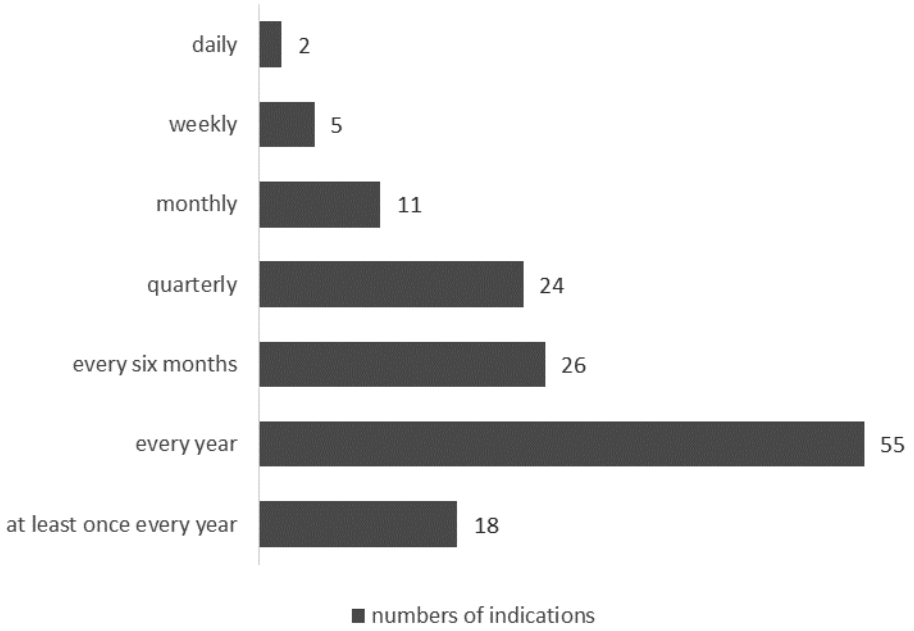

Figure 6. Frequency of the security reviews

Officials evaluated the information security level of its units. Among the 146 answers, 4 rated the level as very good, 95 rated as good, 45 – average, one municipal office rated the level as bad and one official did not have opinion.

4. Conclusion

On the basis on the results of the research it can be concluded, that not all surveyed offices have implemented tasks arising from information security regulations.

It is unacceptable that three years after the introduction of the Regulation of Polish Council of Ministers regarding to the National Interoperability Framework, containing minimum requirements for public registry and information exchange in electronic form and the minimum requirements for ICT systems in some units information security administrators have not been appointed and information security policies have not been implemented.

The results of the survey are consistent with results of the inspections conducted by the Supreme Chamber of Control: "Implementation of selected requirements for ICT systems, exchange of information in electronic form and a National

Interoperability Framework on the example of some offices of municipalities and cities with county rights" [9]. During the inspection Supreme Chamber of Control revealed numerous irregularities and generally negatively assessed the authorities' actions in the field of information security management. According to data from the inspection report among 24 of units surveyed in 21 irregularities were found in the area of information security management. Offices, did not have a comprehensive information security policy, improperly managed the privileges of users did not perform annual internal audits of information security and did not have the required agreements for the purchase or service hardware/software containing provisions guaranteeing the confidentiality of processed data they contain. According to the Supreme Chamber of Control opinion, offices did not pursue the tasks arising from § 20 of mentioned regulation.

Based on the responses obtained from the offices it can be concluded that there is a need for employees training (20 units did not conduct trainings of implemented information security policies, 34 units did not conduct training in information security, information systems security, data protection). Officials also need support in implementing an ISMS. Unfortunately, according to the research, such support could count only 10 offices.

Based on the responses obtained from the offices in which the information security management systems is implemented, key success factors have been identified to implement the ISMS. These include especially:

- allocation of adequate financial resources,
- substantive preparation of employees,
- involvement of the top management,
- employees awareness of the need to ensure the security of information.

Therefore, in order to achieve the successful implementation of an ISMS it is necessary to devote adequate resources from the budgets of municipalities to manage information security. Appropriate ISMS will reduce the risk of information security incidents occurrence and the cost its implementation will certainly be lower than the amounts stolen by cybercriminals.

It is important to continue raising awareness for employees of all levels of the organization and their respective substantive preparation. This can be achieved through the participation of officials in various training courses in the field of information security.

In the context of further research, survey in the district offices is planned.

REFERENCES

[1] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

[2] Korzeniowski L. F. (2012) *Podstawy nauk o bezpieczeństwie*, Warszawa: Difin (in Polish).

[3] Lisiak-Felicka D., Szmit M. (2012) *"Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland*, [in:] Biały W. Kaźmierczak J. (ed.), Systems supporting production engineering, PKJS, Gliwice, pp. 133-145

[4] Lisiak-Felicka D., Szmit M. (2013) *Wybrane aspekty zarządzania bezpieczeństwem informacji w urzędach marszałkowskich*, Securitologia 2/2013, pp.39-53 (in Polish).

[5] Lisiak-Felicka D., Szmit M. (2014) *Information security incidents management in marshal offices and voivodeship offices in Poland*, Studies & Proceedings of Polish Association for Knowledge Management, Volume 72, Bydgoszcz, pp. 28-38,

[6] Lisiak-Felicka D., Szmit M. (2014) *Information Security Management Systems In Marshal Offices In Poland*, „Information Systems In Management", vol. 3(2)/2014, pp. 134-144.

[7] Lisiak-Felicka D., Szmit M. (2014) *Selected Apects of Information Security Management in Voivodeship Office in Poland*, „Securitologia" 2(20)/2014 pp. 55-69.

[8] Monarcha-Matlak A.(2008) *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Polska, pp. 239-268 (in Polish).

[9] NIK, Informacja o wynikach kontroli: *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu*, luty 2015, https://www.nik.gov.pl/kontrole/P/14/004/ [2015-10-17] (in Polish).

[10] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie *dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. 2004 nr 100 poz. 1024) (in Polish).

[11] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie *Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. 2012 poz. 526) (in Polish).

[12] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 r.*, Warszawa 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [2015-10-17] (in Polish).

[13] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, Warszawa 2014,

http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html [2015-10-17] (in Polish).

[14] Suchorzewska A. (2010) *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer Polska, pp. 279-285 (in Polish).

[15] Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 1997, Nr 133, poz. 883, z późn. zm.) (in Polish).

[16] Ustawa z dnia 8 marca 1990 r. *o samorządzie terytorialnym* (Dz.U. 1990 nr 16 poz. 95 z późn. zm.) (in Polish).

[17] https://zaufanatrzeciastrona.pl/post/haslo-do-systemu-wyborczego-na-stronie-urzedu-ty-tez-mogles-testowac/ [2015-10-17] (in Polish).

[18] http://piotrkowtrybunalski.naszemiasto.pl/artykul/dane-osobowe-wyciekly-z-urzedu-miasta-w-piotrkowie,3299451,art,t,id,tm.html [2015-10-17] (in Polish).

[19] http://nowosci.com.pl/340123,Ofensywa-urzedu-po-ataku-hakerskim-Beda-kolejne-zabezpieczenia-strony.html [2015-10-17] (in Polish).

[20] http://nowosci.com.pl/339942,Hakerzy-przejeli-oficjalna-strone-internetowa-Urzedu-Miasta-w-Toruniu.html [2015-10-17] (in Polish).

[21] http://twojepajeczno.pl/wiadomosci/zlodzieje-okradli-gmine-pol-miliona-zlotych/ [2015-10-17] (in Polish).

[22] http://technowinki.onet.pl/aktualnosci/rzeczpospolita-cyberprzestepcy-okradaja-polskie-gminy/8flgkn [2015-10-17] (in Polish).

[23] http://www.spidersweb.pl/2015/10/policja-polsilver-torepublic.html [2015-10-17] (in Polish).

[24] https://zaufanatrzeciastrona.pl/post/urzad-miejski-w-jaworznie-okradziony-na-milion-zlotych/ [2015-10-17] (in Polish).