INFORMATION SECURITY AUDIT IN A COMPANY

Łukasz KISTER *)

ABSTRACT

At present we all are in the center of an evolution of civilization, which transforms from industrial into information one. In the modern world, that some people call - an informational world, business has entered in a new era – era of economy based upon information. That is why the most important assets in a modern company are immaterial stores. Position of a company is strongly related to them. Therefore, it is the very essential task, given to executives by the senior management, to treat the information with particular care. The only tool, that allows to assess real level of the information security is an audit. A properly performed audit let us determine true condition of our information assets and their security.

Key words: Security, information, company, audit

ABSTRACT

Obecnie jesteśmy w centrum wydarzeń ewolucji cywilizacyjnej, która z przemysłowej przekształca się w informacyjną. We współczesnym świecie, przez wielu nazywanym informacyjnym, biznes wkroczył w nową erę – gospodarki opartej na informacji. Dlatego też najważniejszym aktywem współczesnych przedsiębiorstw są ich zasoby niematerialne. To od nich zależy pozycja instytucji. Tak więc dbałość o posiadane zasoby informacyjne staje się podstawowym zadaniem stawianym kadrze menadżerskiej przez najwyższe kierownictwo instytucji. Jedynym narzędziem pozwalającym rzetelnie ocenić poziom bezpieczeństwa informacji jest audyt, który poprawnie przeprowadzony pozwala na ustalenie stanu faktycznego zasobów informacyjnych i ich ochrony.

Key words: Security, information, company, audit

*) Łukasz KISTER, Master of Arts, PhD Students of Department of Security Management Faculty of Special Engineering University of Zilina, Head of PhD Student Section European Association for Security. E-mail: l.kister@bezpieczneinformacje.pl.

1 INFORMATION SECURITY IN A COMPANY

Information is a transferable immaterial good, that minimizes uncertainty [19, p. 8].

Above mentioned definition is sufficient to show significance (value) of information in the modern world. In this particular case related to a company, the best representation is relation between value of information assets and the rest of assets. Different researches shows, that the ratio may reach even 80%. The conclusion, that may be drawn presents that **market value of the company** (business, political, social) **depends upon value of the data processed in this particular company**.

One of the most important mission of the company is to provide acceptable level of security for possessed information assets, that is to be understood as capabilities to protect them against any losts.

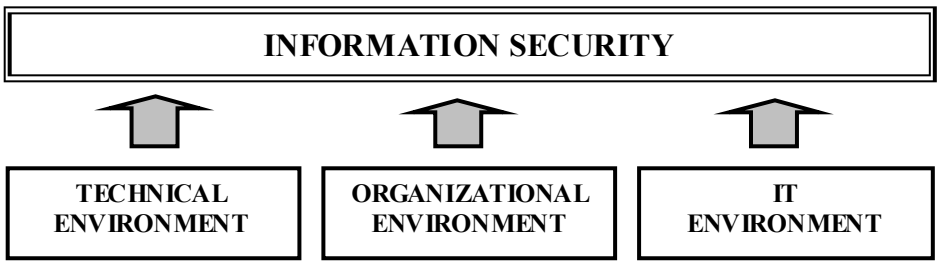

Fig. 1. Elements of information security in a company.
Source: author's own study

To secure information in a company properly is a very complicated undertaking, which requires holistic approach. The first stage is to determine what groups of information are processed in the company and classify them according to the level of confidentiality. Next step is risk assessment for each of the groups made with tools chosen carefully out of three areas: organizational, technical and data computing. **The information security system in the company**, built this way, **will completely achieve all the goals and tasks intended by the company owner**.

2 INFORMATION SECURITY AUDIT

2.1 INFORMATION SECURITY AUDIT DEFINITION

Information security audit is a basic and comprehensive form of analyzing, systemizing and assessing current state of security level of all information processed in the company. The professional and diligent audit allows to prepare a report for the management, that presents, above all, the real state of the information assets and their security.

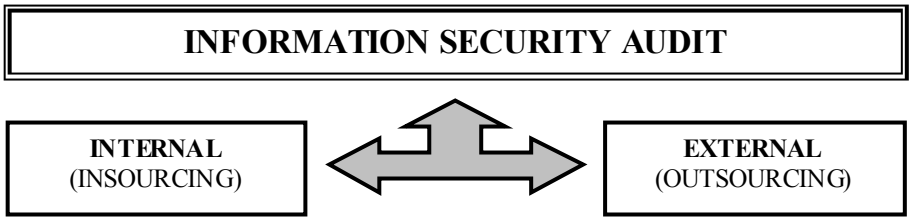

Fig. 2. Division of the information security audit regarding an executive subject. Source: author's own study

The audit may be executed in two forms: **internal** or/and **external audit**. In the first case audit is executed by employees of the company, in the other one execution is commissioned to an specialized external consulting firm or a group of independent experts. Multidisciplinary nature of the information security and necessity of impartial assessment substantiate a choice of external audit in the company.

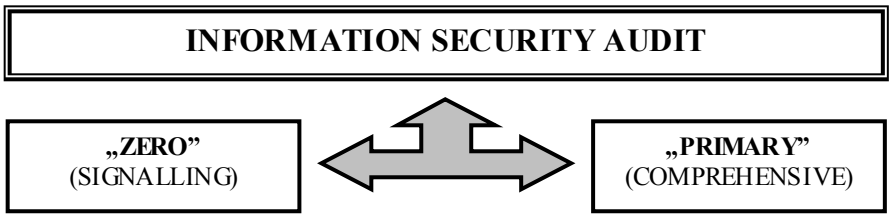

Fig. 3. Division of the information security audit regarding range of the audit. Source: author's own study

Regarding range and detail of researches, audits are divided into: **"zero"** and **"primary"**. The first one is basic (signaling) form of analysis and assessment of management and security of information processed in the company. The only goal of this form is to answer the question whether the company provides acceptable level of information security, without assessing separate elements. The second one is comprehensive and detailed analysis of every element in the information security system of the company.

2.2 RANGE OF RESEARCH

Professional assessment of the information security in the company requires comprehensive analysis of all elements of the information system. In practice, it's assumed, that audit is to cover in this range at least:

1. **Inventories of assets and threat assessment.**
2. **Recognition of organizational structure and areas of security.**
3. **Analysis of physical security in the company.**
4. **Assessment of operational security and internal procedures for securing interests of the company.**
5. **Analysis of computer system security and its infrastructure.**
6. **Analysis of compatibility of existing systems, procedures and policy in relation to the current legal conditions.**

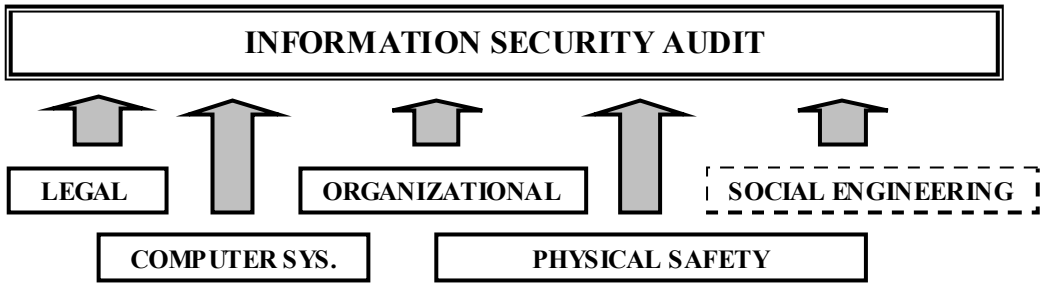

Fig. 4. Division of the information security audit regarding an object of research. Source: author's own study

In order to make research more effective as well as getting results of the analysis easier, auditors should use **unified assessment sheets** and above all clearly specified **threshold of acceptable threats** (negligence).

2.3 AUDIT REPORT

A properly performed audit is to be concluded by a written report, that shows **true condition of all information assets and their security** to the senior management (board, owners).

The audit report is supposed to be a formal document, that meets all standards determined in the company policy for important value documents, especially documents with "sensitive" content. Taking above mentioned under consideration the report usually contains elements listed below:

1. **General information about the audit and the audited company.**
2. **Description and assessment of current state.**
3. **Conclusions and recommendations (key).**

Despite level of detail, the audit report always covers the analysis of weak and strong points of the information security system therefore it is to be classified at the highest level. In practice, access to the report and knowledge about its existence as well ought to be limited for its authors and the senior management only.

3 SCIENTIFIC SUPPORT FOR INFORMATION SECURITY IN A COMPANY - CONCLUSION

Information security in business as an objective of research is located inside an area of interest of many scientific disciplines and their representatives. It might be divided into different groups according to goal, methodology, area of research and its result. The following scientific disciplines support the information security: **legal science** [e.x. 20], **sociology** [e.x. 1], **exact sciences** [e.x. 16], **management** [e.x. 17], **computer science** [e.x. 18], **political science** [e.x. 22], and also: **police science** (public safety and law enforcement) [e.x. 2], **military science** (military art and

military and national security) [e.x. 13] and even **philosophy** (ethics) [e.x. 11] or **physical culture** [e.x. 7].

Above mentioned areas of science do not consider wide spectrum of factors, that may generate different types of threat and influence informational assets in the company. This state created a new discipline of science, that concerned security of human and social organizations – **securitology**. It concerns in its research multisource threats based on: objective and subjective factors, social and psychological factors, culture, political and legal factors, environmental and technical factors, macro and micro economy [e.x. 3,4,5,6,10,12,14,21].

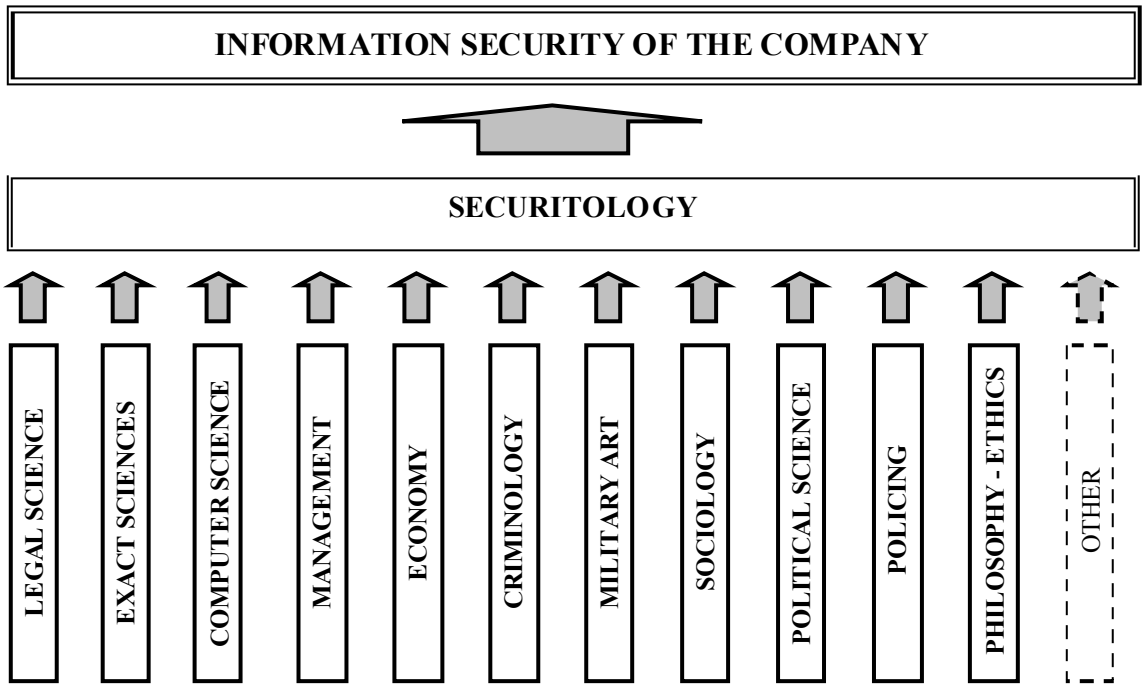

Fig. 5. Scientific support for the information security.
Source: author's own study

Contemporary dimension of security and especially information security in a company clearly confirms need for holistic perspective and strong cooperation among experts and scientists.

REFERENCES

[1] BULLER L.J.: Influencja. Stalowa Wola: KUL, 2008.
[2] DWORZECKI J.: Podstawy prawne wykonywania zadań ochrony osób i mienia. Wybrane zagadnienia. Gliwice: GWSP, 2009.
[3] HOFREITER L.: Securitologia. Liptovský Mikulaš: AOS, 2006.
[4] HOFREITER L.: Bezpečnosťná veda na počiatku milenia. In Bezpečnosť a bezpečnostná veda. Zborník vedeckých a odborných prác. HOFREITER L. (red.). Liptovský Mikuláš: AOS, 2009, s 13-20.
[5] JANOŠEC J.: Sekuritologie – nauka o bezpiečnosti a nebezpiečnosti. „Vojenske rozhledy", 2007, nr 3.

[6] JANOŠEC J.: *Bezpečnosťní realita – předmět Sekuritologie*. In *Bezpečnosť a bezpečnostná veda. Zborník vedeckých a odborných prác*. HOFREITER L. (red.). Liptovský Mikuláš: AOS, 2009, s 27-32.
[7] KAGANEK K.R., KORZENIOWSKI L.F.: *Jakość i bezpieczeństwo usług hotelarskich*. Kraków: EAS: 2008.
[8] KISTER Ł.: *Significance of information security in a company*. In *Riešenie krízových situácií v špecifickom prostredí*. Žilina: Žilinska univerzita, 2009. s. 329-334.
[9] KORZENIOWSKI L.: *Firma w warunkach ryzyka gospodarczego*, Wydanie 2. Kraków: EAS 2002.
[10] KORZENIOWSKI L.F.: *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS 2008.
[11] LIPIEC J.: *Etyka ochrony*. In *Bezpečnosť a ochrana majetku*. Košice: Liport LFK, 2001. s. 82-94
[12] MACIEJEWSKI J.: *securitologia – uwagi socjologa. Bezpieczeństwo w kontekście społeczno-kulturowym*. In *Bezpečnosť a bezpečnostná veda. Zborník vedeckých a odborných prác*. HOFREITER L. (red.). Liptovský Mikuláš: AOS, 2009, s 53-58.
[13] MIKA J.: *Information Warfare and Internet – Strategic problem of future*. In *Internet, competitiveness and organisational security in knowledge society*. [CD-R]. Zlin: Tomas Bata Univeristy in Zlin, 2007.
[14] OHRIMENKO S.: *Зкономика Секюритологии*. In *Bezpečnosť a bezpečnostná veda. Zborník vedeckých a odborných prác*. HOFREITER L. (red.). Liptovský Mikuláš: AOS, 2009, s 71-78.
[15] PIPKIN D.L.: *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*. Warszawa: WNT, 2002.
[16] REITŠPIS J. a kol.: *Manažerstwo bezpiečnostnych rizik*. Žilina: Žilińska univerzita v Žiline, 2004.
[17] STONER J.A.F., FREEMAN R.E., GILBERT D.R., JR.: *Kierowanie*. Warszawa: PWE, 1997.
[18] SZMIT M., GUSTA M., TOMASZEWSKI M.: *101 zabezpieczeń przed atakami w sieci komputerowej*. Gliwice: Wydawnictwo Helion, 2005.
[19] SZPOR G.: *Pojęcie informacji a zakres ochrony danych*. In Fajgielski P. (red.): *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*. Lublin: Wydawnictwo KUL, 2008. s. 7-20.
[20] SZWAJA J.:, *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*. Warszawa: Wydawnictwo C.H.BECK, 2006.
[21] TOMASZEWSKI J.: *Securitologia – próba zdefiniowania nauki*. In *Bezpečnosť a bezpečnostná veda. Zborník vedeckých a odborných prác*. HOFREITER L. (red.). Liptovský Mikuláš: AOS, 2009, s 93-100.
[22] ZALEWSKI S.: *Dylematy ochrony informacji niejawnych*. Katowice: KSOIN, 2009. ISBN 83-922648-5-1

článok recenzoval:
Ing. Tomáš Loveček, PhD.