[w:] Domańska-Szaruga B., Stefaniuk T. (edit.), ***Organization in changing environment Conditions, methods and management practices***, SudioEMKA, Warszawa 2014, ISBN: 978-83-64437-19-9 , ss: 181

CHAPTER VI

Information security in organization in the Knowledge-based Economy

Tomasz Stefaniuk [96]
Bogusz Mikuła[97]

In the past few years, we already got used to the messages about information security violation incidents. The observed social conflict around ACTA with uncomfortable attacks on government services and "Basia's" speech on the Prime Minister websites, as well as a number of serious attacks on companies such as Sony, Oracle, Adobe, Microsoft and Google disproved myths about systems security.[98]

Self-replicating virus shamoon infected 30,000 Windows-based machines of computer network of Saudi Aramco and deleted data from their hard drive. Despite its vast resources as Saudi Arabia's national oil and gas firm, Aramco, according to reports, took almost two weeks to recover from the damage.[99]

Another, even more dangerous virus - Stuxnet that has infected nuclear installations in Tehran, delayed Iran's nuclear program by two years. As experts note, that cyber attack was so effective as a military strike, and even better, because it did not cause loss of human lives or war. The level of complexity of the virus indicates that Stuxnet could arise only through the cooperation of several countries and its development proceeded for a years[100].

[96] PhD, Siedlce University of Natural Sciences and Humanities
[97] Professor, Cracow University of Economics
[98] For example, the attack on Sony ended data leakage about 70 million users, and hacking into Adobe resulted in more than 150 mil lion rows of data (the list of accounts, e-mail address and password protected), which fall into the wrong hands (After:Największe zagrożenia dla bezpieczeństwa Internecie w roku 2013 – Raport, Fundacja Bezpieczna Cyberprzestrzeń, p. 6-7).
[99] http://www.infosecurity-magazine.com/view/29750/shamoon-was-an-external-attack-on-saudi-oil-production
[100] http://www.przeglad-tygodnik.pl/pl/artykul/podstepny-stuxnet

Disclosed details of the Mandiant report[101] about hacking to the databases of organizations operating primarily in the U.S., Canada and the UK by representatives of China, and finally Edward Snowden's sensational information including government PRISM program of the June 2013 years have made, that issues of constantly growing threat to the security of information have become perceived not only by specialists.

In search of answers to the question about the reason for the continuous increasing the amount of incidents related to the information security violation is worth to paying attention to the constantly increasing role of knowledge and information in the global economy. Relying competitive advantage in every area of life on knowledge (both in the economy, the military, medicine or sports) results an increase in its value, and that increase in the value leads to more risks associated with its security.

6.1. Knowledge-based economy and being its consequence overall threats

The last years of the twentieth century brought in a global economy realization of new, different from the occurring, conditions and trends.

The new conditions characterizing the economy meant that it began to be defined as the "new economy", and later used the term "knowledge-based economy", which has been widely adopted in the economic world.

Probably the first time the concept of "knowledge-based economy" was defined in the report of a study conducted by the OECD The Knowledge-based Economy in 1996, recognizing it as the economy which are "directly based on the production, distribution and use of knowledge and information"[102].

Today as a one of the most apropriate terms of the knowledge-based economy is using the the OECD and the World Bank definition where it is considered as the economy, in which "knowledge is created, acquired, transmitted and used effectively by companies, organizations, individuals and community. It is not narrowly focused on high technology industries and ICT, but rather creates a framework to analyze the range of policy options in education, infrastructure and innovation systems that can help initiate the knowledge economy"[103].

The advent of the conditions of knowledge-based economy (KBE) has become for many companies a chance for development, but also has brought a lot of new threats. They result mainly from the basic qualities the KBE:

---

[101] In the report, released 19 feb.2013 by Mandiant, identifed particular group of cybercriminals from China which is blamed for stealing "hundreds of terabytes of data from at least 141 organizations" since 2006, including 115 targets in the U.S. Twenty different industrial sectors were targeted in the attacks: from energy and aerospace to transportation and financial institutions. (http://abcnews.go.com/Blotter/mandiant-report-fingers-chinese-military-us-hack-attacks/story?id=18537307).

[102] M. Cielemęcki, *Gospodarka oparta na wiedzy jako nowy paradygmat rozwoju współczesnych organizacji*, [in:] M. Cisek i B. Domańska-Szaruga (eds.), *Zrównoważony rozwój przedsiębiorstw*, Wydawnictwo Studio Emka, Warszawa 2010, p. 95.

[103] Ibidem, p. 95.

- treating knowledge as a primary production factor, which is the base of rational use of other factors - labor, land and capital - has resulted that many organizations introduced significant changes in the modes of action. The changes consisted inter alia on the purchase and use of modern machinery, specialized computer systems, implementation of knowledge management systems, restructuring of employment and a whole range of organizational changes that have perfected their functioning. However, the creation of a knowledge-based organization carries a risk: in the necessity of incurring large capital expenditures that with lack of proper accuracy, lack of adequate discharge his obligations to business partners, or instability in the financial markets, may lead enterprises to loss of financial liquidity and his fall;
- globalization, which opens up new markets in the world by creating facilitate when purchasing raw materials and intermediates or selling their products, but also intensifies the competition of businesses in the market (also local), creating new spaces for foreign companies;
- the networking, which are consequence of the development of cooperative systems and globalization increasing, which promotes better use of their enterprises abilities, concentration of financial capital, but by the formation of strong economically groups it threatens the existence of small and medium-sized businesses, which are the base of the economy and labor markets especially in developing countries up;
- the turbulence, which is creating unpredictability and chaos;
- increasingly wider use of computer technology in business and in many other spheres of life of societies, that brings many benefits, but also creates a lot of threats like: viruses locking systems, malicious software that obtain private data from the Internet users' computers, etc. Irregular development of electronic economy favors the emergence of phenomena of various kinds of exclusions;
- changes in societies expectations and lifestyles, which creates a demand for many new groups of products and services, but also a whole range of threats, such as a decrease in the level of fertility rate in highly developed societies, increasing the number of divorces, isolation of individuals in community and establishing contacts only with the use of modern means of communication, the growth of various types of addiction and the development of new social pathologies, etc.

In summary these very general and casually presented hazards it should be noticed, that the main danger stemming from the modern economy towards enterprise is widely understood unpredictability.

6.2. Information and knowledge in business and in the economy

Information and knowledge accompany every economic process and determines its efficiency. There are also resources which are involved in the management

process, as a participants in the process of planning, organizing, motivating and control. Information and knowledge are the modern economic resources that allow to reduce the level of uncertainty and the level of unpredictability of the future.

Therefore they have at the present great importance, and an expression of concentration on them special attention are the conceptions of information management and knowledge management.

One of the attempts to distinguish between information and knowledge through the concept of "data" presented DJ Skyrme. According to him, data this are the facts and figures without context (such as sky, 41565), the information consist of the data presented in a specific context (eg a completely overcast sky speed of 130 km / h), while knowledge are the informations having a specific meaning (such as my experience shows that such weather can cause serious delays airplanes). Knowledge leads to wisdom (intelligence), generally perceived as the whole of knowledge and skills of use this knowledge (eg I book a train ticket before other passengers will use this alternative) [104].

This easy distinguish of two characterized economic resources allows to conclude that - in western terms - information is an element of knowledge. Therefore, in practice, information management should be tightly integrated with knowledge management, and from the information quantity and quality depends the quality and quantity of knowledge.

Looking at knowledge resources from the macroeconomic level, L. Zienkowski making a global assessment of the results of model econometric analyzes, infer, a significant impact of knowledge capital on economic growth in the long term the country, no effect of short-term and significant impact in the medium term, however dependent on coexistence of other factors, such as investment in fixed assets and the openness of the economy (the transfer of modern technology and the absorption of knowledge)[105].

The importance of information and knowledge in the economy and business is increased with the organization growth and the volatility and complexity of the economic environment. This resources constitute a necessary basis for rational decision-making, without which we can't talking about the successes and economic development of the country, as well as individual companies.

When we are focusing on the microeconomic level, it should be noted that the gathering of information and knowledge resources in the enterprise, which are appropriate in terms of quantity and quality, necessitates conducting many costly projects through a long period of time. Possession of these resources can be a source of sustainable competitive advantage. Additionally they are more valuable, if it is more difficult to imitate them. Therefore, businesses limited or even protected access to them. However, the situation in this area is not easy. Today, in a substantial part of the work on information and knowledge resources, are used computers connected with the Internet. This gives the possibility of unauthorized acquisition of infor-

[104] D.J. Skyrme, *Knowledge Networking. Creating the Collaborative Enterprise*, Butterworth Heinemann, Oxford 1999.

[105] L. Zienkowski, *Czy kapitał wiedzy oddziałuje na wzrost gospodarczy – spojrzenie ekonomisty*, „Przegląd Socjologiczny", Vol. LVII/3/2008, p. 19.

mation and knowledge by entities desiring them. It is not necessity to explain in detail how valuable can be to stakeholders the informations contained in the personal computer:

- Official's who is finishing work on the zoning plan,
- A marketer who is working on the promotion campaign for a new product group
- Chief technologist having technical documentation about breakthrough technology of some product,
- A scientist who working on a new application of a raw material,
- Analyst who terminating a financial statement of large listed companies, etc.
- Therefore, the importance of information security increases significantly: not only this information which are processed by specialized computer systems, but also recorded on small personal computers.

6.3. New information security threats in the knowledge-based economy

Organizations in the Knowledge-based Economy employ technology and ubiquitous connectivity to share an unprecedented volume of knowledge and information assets with customers, service providers, suppliers, partners, and employees. The sophisticated technologies enable organizations to perform business tasks with a velocity and degree of efficiency that are unprecedented[106]. But risks associated with information security can disrupt operations and even destroy businesses. For this reason, information security is a critical factor for organizations in the knowledge-based economy. In last years, information security threats have changed and have become more common than ever before.

The results of a global survey indicates that the number of security incidents increased in 2013 more than 25% compared with the previous year.[107]

According to an international study which involved 676 IT and IT security practitioners with involvement in endpoint security, the greatest risks to the organization are increased mobility and public cloud computing services (figure 6).[108]

Since the 2012 study was conducted, the percentage of respondents who identified the use of cloud computing resources as a major concern has increased from 28 percent to 44 percent. Fifty-five say the increased use of mobile platforms is a threat to the organization, up from 47 percent last year.

The data in the knowledge-based economy are increasingly distributed and shared between many partners, suppliers, contractors and customers. There are used systems to provide remote access to knowledge and information, as well as mobile devices such as smartphones and tablets, as well as the "bring your own device" (BYOD) trend. While the use of mobile devices to share and transmit data continues

[106] The Global State of Information Security® Survey 2014, PWC, 2014, p.2
[107] Bezpieczne informacje– bezpieczna przyszłość. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2014", p.11 ww.pwc.pl/bezpieczenstwo-biznesu
[108] 2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City, p. 4

to increase, deployment of mobile security policies lags the proliferating use of smartphones and tablets. Based on data and interviews with experts, here are the top five mobile device threats[109]:

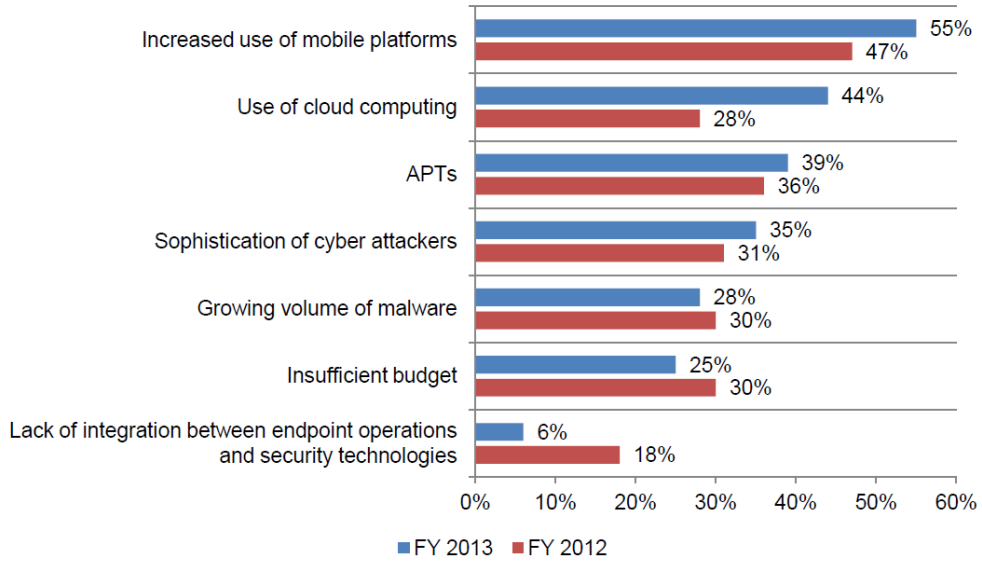

Figure 6. IT security risks of greatest concern to the organization
Source: 2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City, p. 4.

Lost and stolen phones. Symantec researchers left 50 phones behind in different cities and found that 83 percent of the devices (PDF) had corporate applications accessed by the person finding the phone. The challenge is that there is relatively easy techniques for evading some of the on-device security controls, such as bypassing a lock screen password.

Insecure communications. While there is a lot less data on how often mobile users connect to open networks, companies consider insecure connections to wireless network a top threat, Rapid7's Sreenivas says. The problem is that wireless devices are often set to connect to an open network that matches one to which it had previous connected. A lot of people will look for a WiFi hotspot, and they won't look to see if it is secure or insecure," he says. "And once they are on an open network, it is quite easy to execute a man-in-the-middle attack."

Leaving the walled garden. Users who jailbreak their smartphones or use a third-party app store that does not have a strong policy of checking applications for malicious behavior put themselves at greater risk of compromise. If some user are making the decision to download an app from an unknown source in a third-party app store, you are opening yourself up for the potential of malware.

Vulnerable development frameworks. Even legitimate applications can be a threat to the user if the developer does not take security into account when developing the application. Vulnerabilities in popular applications and flaws in frequently used programming frameworks can leave a device open to attack.

[109]http://www.darkreading.com/mobile/4-mobile-device-dangers-that-are-more-of/240161141

Malicious And Suspicious Software. According to the McAfee Labs', mobile malware will drive growth in both technical innovation and the volume of attacks in the overall malware market. That prediction is based on the last two quarters of 2013, which saw new PC malware unchanged and Android samples growth of 33 percent. Because of this, ransomware is expected to blossom as more people and businesses shift over to mobile. Attacks will likely target vulnerabilities in NFC (near field communication), and in the form of compromised valid apps.[110] The number of malicious software and applications that are dangerous for users Android, exceeded 1 million.[111]

Another great risk to data security is cloud computing[112],which has been around for more than a decade, and has simultaneously transformed business and government. Cloud computing has made knowledge and information available in the organization, without spacetime limitation. Almost half (48%) of respondents from Poland use some form of cloud computing. The development of the cloud service model delivers business-supporting technology more efficiently than ever before, but also created new security challenges. Experts identified the following nine critical threats to cloud security (ranked in order of severity)[113]:

1. Data Breaches.
2. Data Loss.
3. Account Hijacking.
4. Insecure APIs.
5. Denial of Service.
6. Malicious Insiders.
7. Abuse of Cloud Services.
8. Insufficient Due Diligence.
9. Shared Technology Issues.

While cloud computing threat is become easier to detect and diffuse simpler and higher-volume attacks, concerns about advanced persistent threats (APT)[114] - targeted attacks that attempt to breach a specific company's data over time - have risen from 14 percent in 2009 to 39 percent in 2013, an increase of 55 percent, according to the Ponemon and Lumension study.[115]

The general trend indicates that in the future APT may constitute a large part of all the risks. In The Global State of Information Security® Survey, hackers increasingly were nominated as a potential source of attacks, so it seems alarming that

[110] http://www.tomsitpro.com/articles/mcafee-exploit-2014-security-mobile,1-1518.html

[111] Największe zagrożenia dla bezpieczeństwa Internecie w roku 2014 – Raport, Fundacja Bezpieczna Cyberprzestrzeń, s.6-7

[112] Cloud computing is an on-demand service model for IT provision. It means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet.

[113] The Notorious Nine Cloud Computing Top Threats in 2013, Cloud Security Alliance, https://cloudsecurityalliance.org/research/top-threats/

[114] An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term. This infographic details the attack phases, methods, and motivations that differentiate APTs from other targeted attacks.

[115] http://www.proofpoint.com/threatinsight/news-feed/articles/mobile-devices-advanced-persistent-threats-to-be-2014s-top-security-concerns-554901

only 30% of respondents in Poland has implemented safeguards against such risks. For comparison - more than half of the survey respondents globally claims that already apply appropriate remedies.[116]

Increasing the level of security, both traditional and computer, lead cybercriminals to the "weakest link", which is a man. Therefore, we can observe a growing number of attacks aimed at obtaining knowledge and information from individuals within the organization who have unfettered access to them. People from "inside" the organization and trusted partners are the dominant source of incidents in organizations around the world (figure 7).

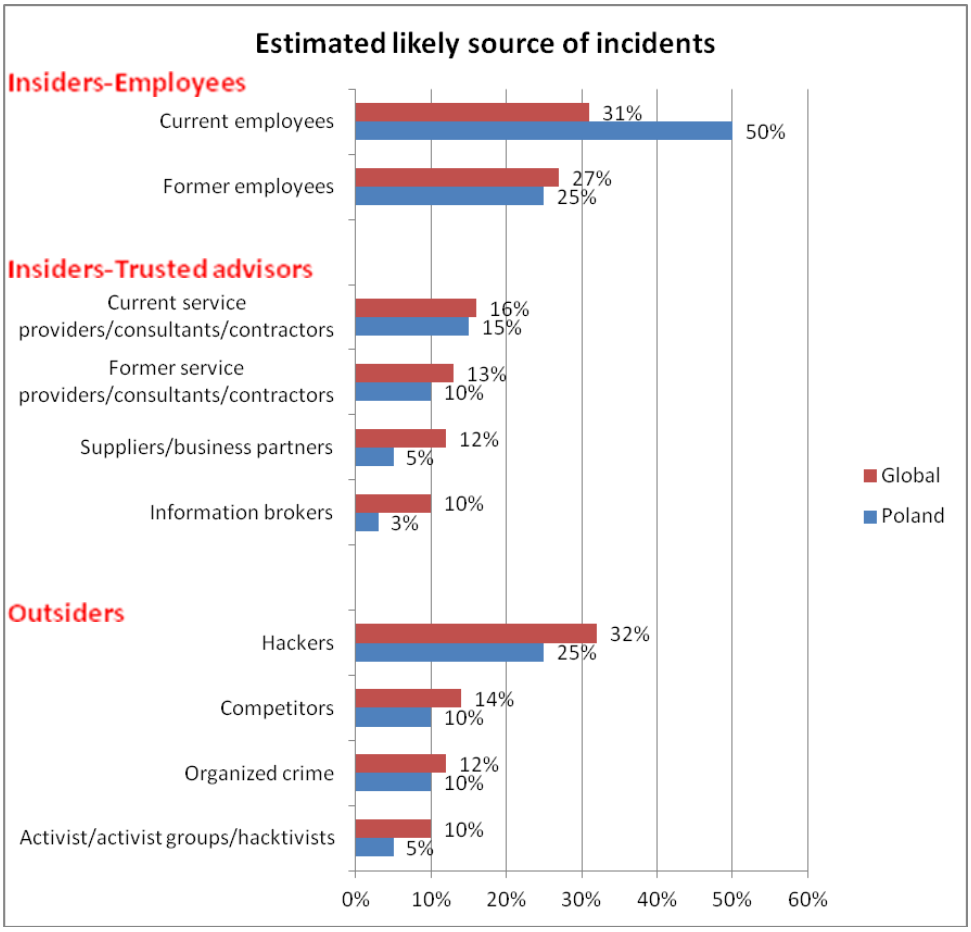

Figure 7. Estimated likely sources of incidents
Sources: Bezpieczne informacje– bezpieczna przyszłość. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2014", p.13, The Global State of Information Security® Survey 2014, PWC, 2014 p. 10.

Special risk is associated middle managers, because they have greater access to information important to the organization than employees in lower positions.

[116] Bezpieczne informacje– bezpieczna przyszłość. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2014", p.16, www.pwc.pl/bezpieczenstwo-biznesu

Man acting unconsciously, or through breaking information security rules may cause to complete discrediting the security system (eg, using "yellow sticky note" of the saved password). Therefore, staff and their IT resources (computers, systems and networks, office, online services) are really just another front, which should include the corporate defenses.The increase in incidents combined with a concurrent rise in the volume of business knowledge being shared digitally results in an unsurprising finding: Proliferating data loss. According to The Global State of Information Security® Survey, in 2013 24% of respondents reported loss of data (in Poland – almost 50%!!!) as a result of security incidents, a hike of 16% over 2012. Delving into the types of data exploited reveals some interesting findings. In almost half the cases, these incidents relate to the brand or reputation. But on the lead the effects of security incidents also were (figure 8).[117]

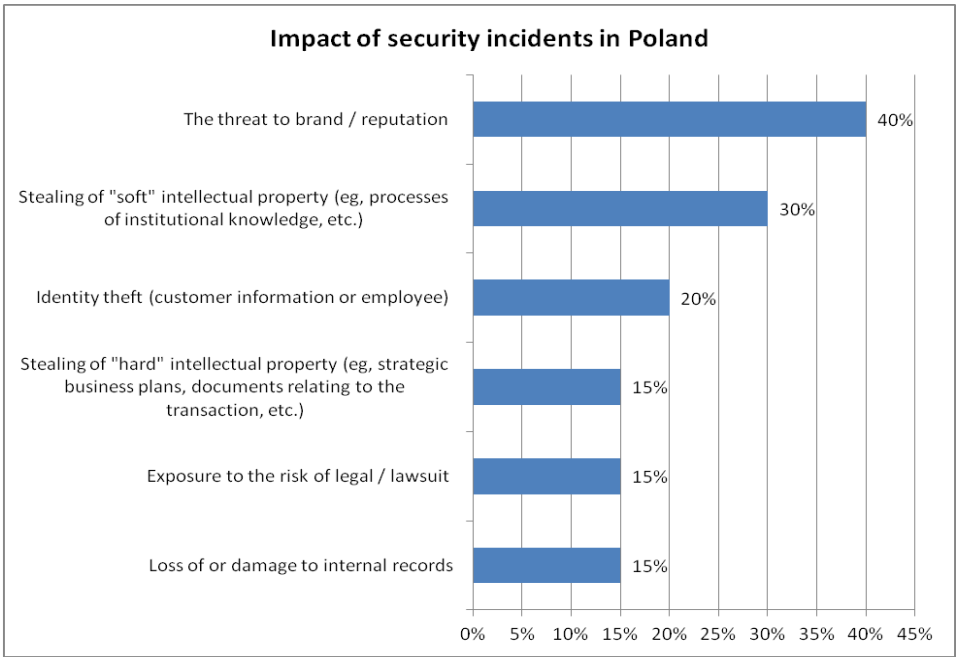

Figure 8. Impact of security incidents in Poland
Sources: Bezpieczne informacje– bezpieczna przyszłość. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2014", p.12, www.pwc.pl/bezpieczenstwo-biznesu

- stealing of "soft" intellectual property (eg, processes of institutional knowledge, etc.),
- identity theft (customer information or employee),
- heft of "hard" intellectual property (eg, strategic business plans, transaction documents, etc.).

However, the survey results indicate that the applied security measures do not allow for an effective fight against the risk of of intellectual property theft .

[117] Bezpieczne informacje– bezpieczna przyszłość. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2014", p.12, www.pwc.pl/bezpieczenstwo-biznesu

6.4. Risk analysis as a key element of creating a security policy in knowledge-based economy

To combat today's risks, organizations should be able to achieve ongoing insight and intelligence on ecosystem vulnerabilities and dynamic threats. Activities and investments should be driven by the best available knowledge about information assets, ecosystem threats, and vulnerabilities—and evaluated within the context of business activity.[118]

The traditional reactive approach to information security strategy, which typically relegates security to an IT challenge, remains commonplace. But it is no longer effective, nor is it defensible. Today's new world of security risks demands that organizations treat information security threats as enterprise risk-management issues that can critically threaten business objectives. Safeguarding all data at the highest level is no longer realistic or even possible.

Risk analysis enables an organization to identify threats and the associated vulnerabilities which have the potential to negatively impact their business. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threats being realized. Therefore risk analysis is a critical element for the management of knowledge and information systems security[119].

Risks are a function of: [120]

- the asset values,
- the threats, and their associated likelihood of the occurrence, that may threaten the assets.
- the ease of exploitation of vulnerabilities by threats to cause unwanted impacts, and
- the existing or planned safeguards, which might reduce the severity of vulnerabilities, threats and impacts

Organizations have many reasons for taking a proactive risk analysis to addressing information security concerns[121]:

Necessity of having an accurate inventory of IT assets as well as data assets and asset value in dollars, the importance of assets to the organization, or their criticality to the organization.

Risks analysis lets identified and documented threats, and known vulnerabilities and prioritized based on impact or criticality of the IT asset or data asset that it impacts.

A risk assessment assists the organization in justifying the cost of needed security countermeasures and solutions to mitigate the identified risks, threats, and vulnerabilities,as well as assists IT organizations with understanding the return on investment if funds are invested in IT security infrastructure.

---

[118] The Global State of Information Security® Survey 2014, PWC, 2014, p. 2.

[119] L.S. Rutgers, R.P. Srivastava, T. J. Mock, *An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions*, [in:] „Journal of Management Information Systems", Vol. 22, No. 4, Spring 2006, p. 107

[120] ISO/IEC TR 13335 – Part 3b, p. 78

[121] http://www.informit.com/articles/article.aspx?p=426764&seqNum=5

Legal and regulatory requirements aimed at protecting sensitive or personal data, as well as general public security requirements.[122]

One of the key elements of ISO 27001 certification involves doing a comprehensive risk assessment.

Risks analysis is the initial point for risks management and can be performed without any useless time investments and investments to sources by the short initial analysis performance of all systems[123].

A comprehensive enterprise security risk assessment also helps determine the value of the various types of knowledge generated and stored across the organization. Without valuing the various types of knowledge in the organization, it is nearly impossible to prioritize and allocate technology resources where they are needed the most. To accurately assess risk, management must identify the knowledge that are most valuable to the organization, the storage mechanisms of said knowledge and their associated vulnerabilities.[124]

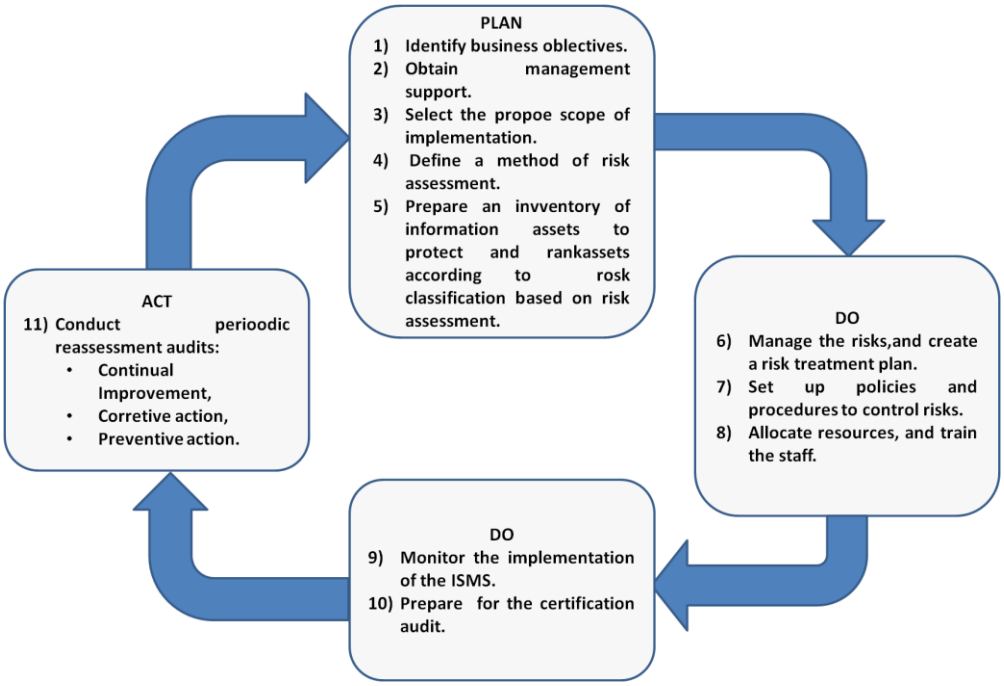

Figure 9. PDCA cycle in information security management system
Source: http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

[122] http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx
[123] O. Strnád, Risk analysis and management of information security, [in:] Transfer inovácií 26/2013, p. 44.
[124] http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx

In particular, risk assessments provide a basis for establishing appropriate security policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected. [125] This continuing cycle of activity, including risk assessment, may be conducted follows the plan-do-check-act (PDCA) cycle (figure 9).

Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing.

Many ISS risk analysis methodologies and standards have been developed by both academic researchers and practitioners, including quantitative methods such as analysis, questionnaire, fuzzy metrics, and popular practical toolkits such as:

- ISO/IEC 27005:2008 - Information security risk management
- CRAMM (CCTA Risk Analysis and Management Method) developed by Central Computer and Telecommunications Agency (CCTA).
- NIST SP800-30 - Risk management guide for IT systems
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) information security risk evaluation
- IRAM (Information Risk Analysis Methodologies) developed by Information Security Forum,

One of the simplest methods of risk analysis described in ISO/IEC TR 13335 – Part 3b, is *the* Ranking of Threats by Measures of Risk. A matrix or table is used here to relate the factors of impact (asset value) and likelihood of threat occurrence (taking account of vulnerability aspects) in the following steps (table 6):

- Evaluation of the impact (asset value) on a predefined scale, e.g., 1 through 5, of each threatened asset (column'b' in the table).
- Evaluation of the likelihood of threat occurrence on a predefined scale, e.g., 1 through 5, of each threat (column 'c' in the table).
- Calculation of the measure of risk by multiplying (b x c).
- Making ranking in order of their ‘exposure' factor.

Table 6. Simple risk assessment table

Asset	**Threat**	**Impact value b**	**likelihood of threat occurrence c**	**measure of risk bxc**
Server	Electricity outage	4	2	8
	Fire	5	2	10
Staff	Loss of key staff	5	2	10
	Accident	3	3	9

Source: Own research

[125] http://www.gao.gov/special.pubs/ai00033.pdf

This procedure permits different threats with differing impacts and likelihoods of occurrence to be compared and ranked in order of priority, as shown here. In some instances it will be necessary to associate monetary values with the empirical scales used here.

6.5. Conclusions

Today's world is constantly changing: is unpredictable, volatile, and seems to become more dangerous every day. In this world information and knowledge are the modern economic resources that allow to reduce the level of uncertainty and the level of unpredictability of the future. They are a necessary base for rational decision-making, without which we can't talking about the successes and economic development of the country, as well as individual companies. Possession of information and knowledge can be a source of sustainable competitive advantage.

Growing importance of information and knowledge has made that has arisen new threats to their safety. Every year we can observe a growing numbers of new threats to the security of information and knowledge, associated with mobility increasing and using public cloud computing services.

In effect, in knowledge based economy, no system, no organization and none knowledge can be absolutely secure.

To ensure the best possible protection for knowledge, organizations should conduct a risk assessment of information security. Through this analysis, it will be possible to create an optimal security system.