A Qualitative Security Model for Business Processes

Dominik Hryszkiewicz
Police Academy in Szczytno, Poland
Barbara Lubas
Nadbużańska Szkoła Wyższa in Siemiatycze, Poland

Abstract. *The aim of this article is to present the situation of Polish enterprises in terms of the protection of data security, as well as identify and highlight the importance of this criterion affecting the management systems of business organisations, and entrepreneurs' approaches to taking action in this regard. The authors present a proposal to create a high-quality security model for securing business processes based on company policies and procedures for information security while maintaining the principle of continuity of operations in respect of business functions. The analyses presented in this article are an independent overview and are based on the findings of the literature and current research in the IT sector using Polish and international databases. The proposed quality model concerning the security of business processes is described and explained. According to the authors, in order to reduce the risk of business disruption, achieve the objectives of compliance with regulations and respond appropriately to complex security breaches, organisations must integrate security structures, constantly monitor the standards adopted, along with rules and control mechanisms, so as to meet the set parameters and remain within the appetite for risk.*

DOI: 10.5604/20805268.1212129
http://dx.doi.org/10.5604/20805268.1212129

Keywords: data security, business processes, business continuity, process management model, information management, protection

Introduction

The increase in sophistication of security measures, mainly in the area of technical security systems, is associated on the one hand with the increase in the value of the resources protected and, on the other hand, is the result of the activity of criminal circles in perfecting techniques used to carry out offences. Enterprises are forced to use more advanced organisational and technical solutions in their security systems but at the same time this results in higher expenditure incurred by the organisations. As one of the elements that determine the competitiveness of companies, the increase in spending on investment in safety is associated with a need to control and optimise it.

This is without doubt a reason to put forward the thesis that the efficient management of enterprises has become necessary to ensure the continuing existence of business organisations, and that security issues, in view of their increasing importance and growing complexity, require the creation of specialised governance structures.

The aim of the article is to present the situation of Polish enterprises, particularly those from the SME sector, in terms of protecting the security of data, show the importance of this criterion for the system of business organisation management and for the approach of entrepreneurs towards taking action in this

respect, as well as to attempt to create a high-quality security model for securing business processes based on a company's procedures for information security while maintaining the principle of continuity of operations in respect of business functions.

Information Security Policy

Having information and a strategic information system is extremely important and necessary for every company because such knowledge, with an appropriate organisational culture, enables effective management of the company. Previously, management of information was aimed at supporting the management of operational processes to reduce costs and increase productivity. It was only at the end of the last century that information management was considered a major factor in the creation and implementation of a business strategy. Today, good business management is the management of its future; that is information management.[1]

We often talk about the need to introduce an effective information security policy, which is clearly and legibly set out and, above all, ensures the security of information systems through IT rules and procedures to enable the correct use of the resources of the entire company.

Information storage is a feature of the system and consists in saving the strategic information on fixed media in a form and formats that are easy to use. This is possible thanks to the operation of cataloguing and creating databases.

The strategic importance of information technology is associated with the concept of information as a strategic resource. It is information that is the basis for creating a strategy and building a potential source of competitive advantage.[2] In order to achieve this, information resources need to be created. Thus a company needs an information strategy defining the information needs and ways of meeting them, and the aim of this strategy is to determine what kind of information should be collected, gathered and stored, and to decide with whom in the e-enterprise and beyond it will be shared. It should also seek to build a system to ensure appropriate and effective creation and use of information.

It is worth quoting here the elements included in the whole process of information management in the enterprise, on which every company incurs costs and takes appropriate action:

a) planning, development and implementation of an information strategy for e-business subordinate to its information policy;
b) information flow control in an e-enterprise communication network;
c) planning of investment resources for the development of information systems;
d) ensuring effective use of IT systems to support decision making;
e) the introduction of new systems, for example, customer relationship management (CRM) systems;

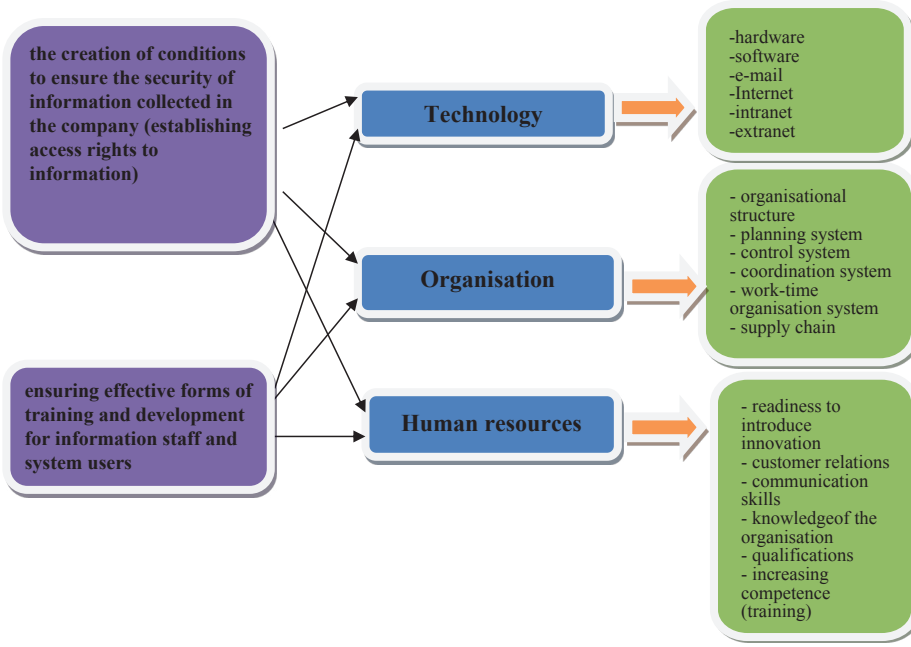
[1] Kotler P, Marketing. Analiza, planowanie, wdrażanie i kontrola, 6th edition. Warsaw: Gebethner i Ska, 1994, p. 38.

[2] Porter M.E, Strategia konkurencji. Warsaw: PWE, 1992, p. 34.

f) information quality management, that is making sure that the information used by management has as many as possible of the attributes of high quality information;
g) the creation of conditions to ensure the security of information collected in the company (to establish access rights to information);
h) ensuring effective forms of training and development of information staff and system users;
i) integration of information systems used at various management levels and in different functional subsystems;
j) designing innovation and adaptation activities;
k) implementation of initiatives aimed at ensuring customer loyalty.[3]

Considering the essence of effective action in the area of information protection and creating appropriate safeguards should start from the system itself ensuring appropriate and effective creation and use of information in the enterprise. Equal weight should also be given to the importance of all elements of security and protection activities in three areas: technology, work organisation and human resources. Bearing in mind the following flow chart (Figure 1), companies should manage information not only in terms of technology as is usually the case, although experience shows this is done in an inadequate way, but there must be visible

Figure 1. Elements of a system for effective action in the field of protection and creation of information security in the enterprise



Source: own

[3] Frąś J, Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa. *Studia i prace wydziału nauk ekonomicznych i zarządzania*, 2011, No. 21, p. 34.

synergies or merging of all three aspects of effective information management presented.

The Situation of Polish Enterprises in Terms of Data Security

The topics concerning the security of business processes are mostly focused around data protection, but mainly in the area of technical security, and this is obviously one of the most important aspects of the functioning of the current security policy of companies. However, looking more broadly at issues of company security systems, equal weight should be given to the issue of organising security systems.

It is appropriate at this point to discuss the situation of Polish enterprises with respect to the importance that they attach to treating security as one of the most important determinants of competitiveness and avoiding the risks of exclusion from the market in the event of emergencies resulting from system failures.

Very often one comes across the statement that small companies do not care about security. Many owners of small businesses in particular assume that, as such, they will not be attacked by hackers. This is definitely the wrong approach, because each company, regardless of its size, is at risk. Very often, a small business is not an end in itself, but is an important link in transmitting data to corporations.

It is true that the potential impact of cyber attacks and the loss of confidential data on business activity are given particular attention in the large organisations. Cyber crime affects not only large corporations or government agencies. More and more often the victims of attacks on the networks are small and medium-sized enterprises. Meanwhile, almost 70% of representatives of small businesses do not believe, or do not know, that a breach of data security will have a financial impact or a negative impact on the credibility of their business. According to the experts Deloitte, small business owners should invest in employee training and develop procedures, the observance of which will ensure the security of the network. Awareness of the impact of network threats on the functioning of the company is often smaller in the case of small and medium-sized enterprises. Indeed, it should be emphasised that the issues of IT security are not a special priority for SMEs because managers cannot form a clear strategy to combat this type of threat.[4]

[4] Based on the report entitled "The Risk of an Uncertain Security Strategy" conducted by the Ponemon Institute on behalf of Sophos. Based on the answers to the 12 questions included in the survey, Ponemon created an "uncertainty index", ranging from 10 (greatest uncertainty) to 1 (no uncertainty). The report confirms that it is US organisations that have the highest rate of the uncertainty of IT threats with a score of 5.9, followed closely by the United Kingdom (5.0) and organisations from the Asia-Pacific region (4.8). The SME sector in Germany has the highest awareness of cyber-threats (3.8). Smaller organisations are the most uncertain of IT threats. Companies with fewer than 100 employees have an assessment of 6.5. According to the survey, the higher the position of an employee in an organisation the greater the uncertainty about the IT security strategy. The directors received a score of 6.8.

The lack of response to the threats exploiting vulnerabilities is worrying. There remains a lack of knowledge about the frequency and scale of cyber attacks and this lack of knowledge prevents the implementation of an effective IT security policy. Moreover, IT security is still not a priority for companies.[5]

It is difficult to find information anywhere on the economic impact of the activities of cyber criminals. It is simply unknown. However, we can hypothetically estimate that the cost of disruption caused by the actions of cyber criminals is much higher than the cost of damage, theft of property and infrastructure. A large number of entrepreneurs cannot estimate the cost of the losses caused by the loss of digital data. One third of small businesses do not have training in the field of data security. Small businesses ignore cyber threats. Data security is low down on the list of priorities of small businesses; as many as 40% of them have not implemented procedures and mechanisms for secure data processing and data destruction.[6]

In relation to similar organisations in the world, Polish companies stand out favourably especially in those areas that require compliance with the restrictive provisions of the law — in particular concerning the protection of personal data and intellectual property. At the same time indicators of the strategic role of cyber security — the position in the company or the size of the budget, significantly deviate from best practice and compare poorly.

In the Polish market, it is clear that the desire to develop information security meets with significant financial constraints. The budget for these activities remains at a low level — it represents only 2.7% of the funds spent on IT. For comparison, worldwide spending on security amounts to an average of up to 3.8% of IT budgets, which are funded at an incomparably higher level than in Poland. The average loss for the company as a result of a security breach across the world is $531. Interestingly, in the last two years, there has been a 50% increase in the number of enterprises with losses of a figure of more than $10 million. This phenomenon also applies to those industries that traditionally invest more in security such as the financial sector, pharmaceuticals and IT.

The most common result of security breaches are loss or theft of data. In Poland, nearly 50% of all attacks end up with leaks or unavailability of information. A similar trend is observed across the world — data loss is a result of 24% of all incidents, 16% more than last year. It is interesting that as many as 42% of respondents worldwide do not use the simplest tools to prevent data loss.

At the same time, although 47% of respondents worldwide use cloud computing, only 18% take into account the rules concerning the cloud in their security policy. The results show that although the majority of respondents implement

[5] For 44% of those surveyed, IT security issues are not a priority. This is evidenced by the fact that 42% of respondents believe that their budget is not sufficient to ensure effective protection of IT. In addition, 26% say that their IT staff have insufficient knowledge to manage security policy. Lack of investment in cyber security: respondents in senior positions have the most uncertainty about the risks in their organisations. Some 58% of the respondents claim that the board does not view cyber attacks as a significant risk.

[6] *Electronic source:* http://www.chip.pl/news/bezpieczenstwo/technologie-bezpieczenstwa/2013/07/male-firmy-lekcewaza cyberzagrozenia#ixzz2uWDqLFgY, *accessed*: 12.01.2015.

the traditional precautions (such as VPN, firewall, encryption, PC), just a few of them use tools that monitor data and networks, enabling analysis of current threats in real time.[7]

Ensuring Continuity of Business Functions

To ensure the protection of continuous processes, the most important things would appear to be the encapsulation of data and the introduction of individual permissions so that whenever the data is to be used each individual operating on the data from different places is the only one with access to their area. However, here too we are not certain, although it is decidedly closer to the truth, that data protection for single systems must be equivalent to the level of security that protects the entire company.

If there is a central database that stores resources such as: customer database, transactions completed, the volume of these transactions or frequency etc, this database needs to be especially secure. Within the totality of the company (all outlets, branches, subsidiaries) access to this database is available to all units.

This raises the question:

How to protect central databases (data processing centres) and how to prevent a loss of continuity of business processes in the company?

Firstly, it is worth considering the overall sensitivity of the central database and assessing how that sensitivity sits on a range from low to high. This consists of determining criteria that increase the level of susceptibility of the database to external and internal attack. The higher the number of indicators the more sensitive the database which should direct the enterprise towards ensuring the best possible technical protection. This is a risk assessment and analysis of the critical factors. Another important aspect is assessing the ability to regenerate and the building of a recovery strategy. This can be called the first stage of the new approach to the construction of a professional model and comprehensive protection of business processes, in which only one of the elements is the protection of data.

Of course, technical protection itself does not guarantee, as mentioned above, information security, but certainly reduces the risk of data loss due to a lack of technical security. We cannot forget that data loss does not occur only with

[7] The report "Information Security — safe future" is based on a global study "The Global State of Information Security® 2014 conducted by PwC and the magazine CIO and CSO magazine. The results discussed in the global report are based on responses given by more than 9,600 managers, among whom were the CEO, CFO, CISO, CIO, CSO, vice presidents and directors of IT and information security from 115 countries. Thirty-six percent of respondents were from North America, 26 percent from Europe, 21 percent from Asia and the Pacific area, 16 percent from South America, while two percent were from the Middle East and Africa. The margin of error is less than one percent. The global survey was supplemented by a Polish section, with contributions from over 70 companies and organisations operating in Poland. The main sectors represented among the Polish respondents were the financial sector (banking and insurance), telecommunications, industry, consulting services and software development.

theft as a motive, but also in the event of a natural disaster or due to intentional or unintentional human activity.

Hard disks included in the database should be fully encrypted to prevent data leakage in the event of physical theft. Such elements as passwords should not of course be stored as clear text but hashed so that, even after the database is extracted, it is impossible to restore these passwords. Data bases should be divided between users so that no one user ever has access to the entire database. This will prevent the leakage of all the resources of the company after the disclosure of database credentials of only one user. Transmission between the main database and its users should also be encrypted to prevent it from being read. The transmission is usually encrypted using symmetric encryption, which is encryption that protects data with a password making it almost impossible to reproduce without its knowledge. However, both parties to the communication process must also know the password to establish transmission using asymmetric encryption, which is based on a method of operation using private and public keys. The password is sent after public key encryption and it is impossible to decipher it without having the private key, which only the transmission recipient has.

If a disaster has already taken place then the most important thing is to ensure the continuity of business processes. This is in fact a requirement of our times, because recovery of the data after the disaster, i.e. rebuilding the centralised Data Centre, is unfortunately no longer enough. It is as if only the second part of the plan to protect the Central Database has been realised, whereas this is not even a protection plan but merely an ability to recover data after a disaster that could have been prevented. It is typical traditional thinking named in the 80's as so called Disaster Recovery, unfortunately still believed in by many entrepreneurs, especially those saving on security, or those who do not even have an awareness of possible consequence of the omission of certain actions in this aspect. While the traditional approach is still important, it proves to be insufficient for the distributed environment. In the Internet environment the requirement for continuous operations takes on a whole new dimension.

If uninterrupted access to information is required, i.e. if the company is not able to function even for a moment without access to software, networks, call centres, etc. since this would entail the loss of clients and customers, resulting in a loss of profits for the enterprise, there is a need to protect against the loss of business continuity through the creation of systems which, even in a crisis, would allow for the efficient handling of these business processes.

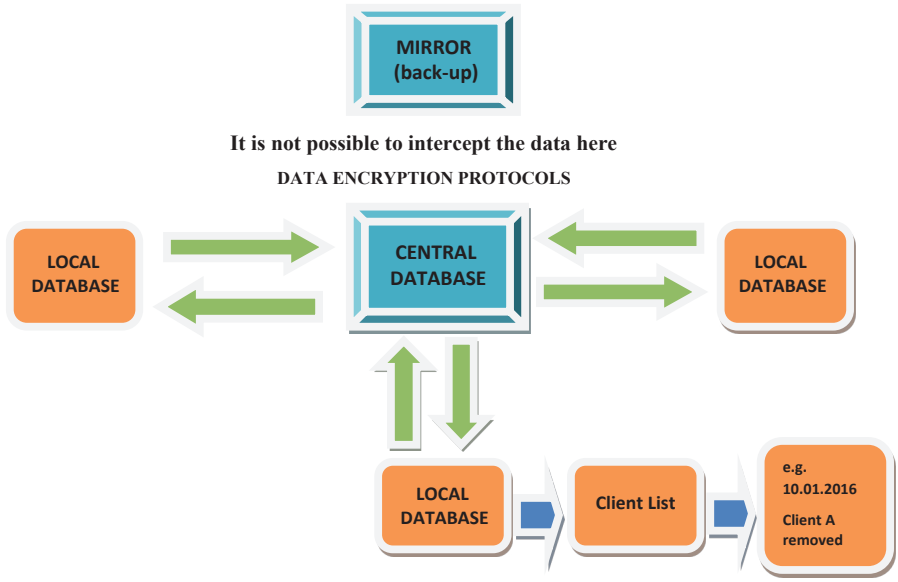
One of the models that can be offered for the continuity of business processes while ensuring data security at the time of interruption of the system, is a centralised model (Figure 2).

This model is based on the existence of a central database that stores all of the resources held by the company. Assuming that the company's headquarters location is the same as the central database, the greatest attention should focus on its security and backing up its data. The best solution to this is to create a number of mirror images of the database, as well as to ensure the ability to restore the database to the state it was in before the failure (disaster recovery), because tens, and in fact sometimes even hundreds, of affiliates and their branches are meant to have immediate access to the resources of the central headquarters whether

or not they all use them at the same time. But in order not to lose the continuity of work, or business processes, each database user needs to create a local copy of the resources they use. In such a situation, in the case of an inability to connect to the central database, a local database is run and all changes that occur during the time of the outage are contained within it.

This model demonstrates how important it has become to protect critical business processes with their complex interdependencies and that it is just as important as data protection.

Figure 2.



Source: own work

Reasons for the Development of a Qualitative Model for the Protection of Business Processes

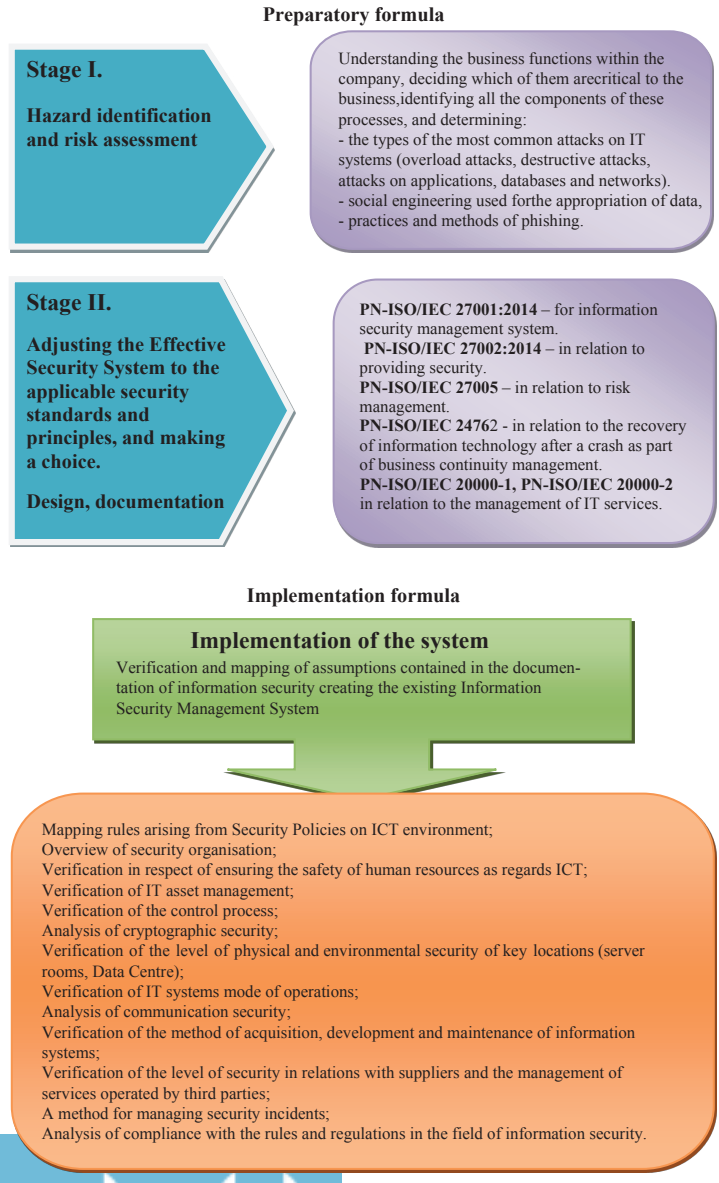
The biggest challenge for companies in the area of security of business processes is threat identification. The need to establish an effective security system is based primarily on a system of information security. The most commonly used standard for determining the current and the required level of information security in a company is the standard ISO 17799 (originally this was the British standard BS 7799), which defines all the relevant aspects related to the protection of information and computer systems. This standard is divided into ten different thematic areas:

- the creation and organisation of security policy within the company,
- rules and procedures for the classification of information resources,
- personnel-related security — the human factor,
- physical security and natural disasters,

- management and maintenance of computer systems and networks
- management of access to systems and information,
- proper maintenance of computer systems,
- planning activities to maintain the continuity of the computer systems,
- compliance with legal and statutory obligations.

Based on the above, an original proposal for a model for implementation of effective information security management in an enterprise has been developed (Figure 3).

Figure 3. Example of a qualitative model for information security management



Companies must continually analyse both the internal and external data flow. As well as this, it is necessary to establish appropriate procedures and rules of conduct and regular training of employees. It is not only necessary to implement appropriate protection measures, but also to develop a business culture which will help counteract potential attacks. It is also extremely important to exchange experiences related to cybercrime in the framework of professional organisations.

Summary

The greatest source of threats to companies are people, followed by data, information and knowledge (as subject and object of business processes), and also cooperating companies. The various sources of risk mutually overlap, as threats often emerge in the area of links of employees with entities and people from outside.

For too long, importance was attached only to the technological aspect, even in cases of data leakage. While it is true that technological problems are one of the main reasons for the disturbances in the flow of information and information security, they are not the only ones. It is also people, organisation, culture and processes.

Enterprises can no longer manage security by acting on an ad-hoc basis. To reduce the risk of interference in operations, achieve the objectives of compliance with regulations and respond appropriately to complex security breaches, organisations must integrate security structures. Companies should constantly monitor the adopted standards, rules and control mechanisms, so as to meet the set parameters.

An effective security policy allows a realistic assessment of the weaknesses, and the use of active protection of information assets. Managing security in a comprehensive manner facilitates compliance with standards and following the rules adopted within the framework of security policy.

References

1. Frąś J, Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa. *Studia i prace wydziału nauk ekonomicznych i zarządzania*, 2011, No. 21.
2. Kotler P, Marketing. Analiza, planowanie, wdrażanie i kontrola, 6th edition. Warsaw: Gebethner i Ska, 1994.
3. Porter M.E, Strategia konkurencji. Warsaw: PWE, 1992.
4. Report „Efektywne zarządzanie bezpieczeństwem informacji", SZiP. *Electronic source:* https://www.us.edu.pl/sites/all/files/www/wiadomosci/pliki/RAPORT 2013.pdf, *accessed:* 16.01.2015.
5. Report "Bezpieczeństwo informacji — bezpieczna przyszłość" was based on a global study — The Global State of Information Security® 2014 (*Electronic source:* http://it.wnp.pl/rosnie-grozba-atakow-itc-na-firmy,213335_1_0_0.html).

About the authors

Cpt. Dominik Hryszkiewicz, *PhD, is the Director of the Institute of Social Sciences of the Faculty of Administration at the Police Academy in Szczytno. His scientific interests include social sciences and public security.* Correspondence*: Wyzsza Szkola Policji w Szczytnie, ul. M. J. Pilsudskiego 111, 12-100 Szczytno, Poland. E-mail: d.hryszkiewicz@wspol.edu.pl*

Barbara Lubas, *PhD, Dr habil., is a coach and academic teacher at the John Paul II Catholic University of Lublin in the field of Management from The International Personnel Academy in Kiev, a professor of this University, and the Dean of Nadbużańska Szkoła Wyższa in Siemiatycze, Poland. Her main scientific interests are management, marketing, psychological and sociological aspects of business administration, quality management, competitiveness of business entities, management in public sector.* Correspondence*: Nadbuzanska Szkola Wyzsza, ul. Kościuszki 43, 17-300 Siemiatycze, Poland. E-mail: barbara_lubas@poczta.onet.pl*

Streszczenie. *Celem artykułu jest przedstawienie sytuacji polskich przedsiębiorstw w aspekcie ochrony bezpieczeństwa danych, wskazanie i podkreślenie wagi tego kryterium wpływającego na system zarządzania organizacji biznesowych oraz podejścia przedsiębiorców do podejmowania działań w tym zakresie. Autorzy przedstawiają propozycję stworzenia jakościowego modelu zabezpieczenia procesów biznesowych opierając się na procedurach polityki bezpieczeństwa informacji firmy przy jednoczesnym zachowaniu reguły ciągłości działania w obszarze funkcji biznesowych. Przeprowadzone w artykule analizy mają charakter przeglądowy i bazują na dorobku literatury przedmiotu, aktualnych badaniach sektora IT polskich i światowych baz danych. Zaproponowany model jakościowy, dotyczący zabezpieczenia procesów biznesowych przedsiębiorstwa, ma charakter opisowy i wyjaśniający. Zdaniem autorów w celu zmniejszenia ryzyka zakłóceń w działalności, osiągnięcia celów zgodności z przepisami i właściwego reagowania na kompleksowe naruszenia bezpieczeństwa, organizacje muszą integrować struktury bezpieczeństwa, stale monitorować przyjęte standardy, zasady i mechanizmy kontroli, tak by spełniały one ustalone parametry i mieściły się w ramach apetytu na ryzyko.*

Резюме. *Целью данной статьи является представление ситуации польских предприятий в сфере охраны безопасности данных, указание и подчеркивание важности этого критерия, влияющего на систему управления бизнес организациями, а также отношение предпринимателей к каким-либо действиям в этой сфере. Авторы представляют предложения по созданию качественной модели охраны бизнес процессов на основе процедур политики безопасности информации фирмы, присоблюдении правила непрерывности действий в сфере бизнес функций. Представленные в статье аналитические выкладки носят обзорный характер и основаны на выкладках из литературы по данной тематике, актуальных исследованиях ИТ сектора польских и мировых баз данных. Предложенная качественная модель, касающаяся безопасности бизнес процессов предприятия, носит описательный и объяснительный характер. По мнению авторов, для уменьшения риска нарушений бизнес деятельности, достижения соответствия правилам и правильного реагирования на комплексные нарушения безопасности организации должны интегрировать структуры безопасности, постоянно проверять принятые стандарты, правила и механизмы контроля, которые должны неизменно соответствовать установленным переметрам и низкой степени риска.*