DE GRUYTER OPEN

International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXI No 3 2015

# ENSURING SECURITY OF DATA USED BY ECONOMIC ORGANIZATIONS FOR DECISION SUPPORT

**Mihai ANDRONIE**

**Spiru Haret University, Bucureşti, România,**
mihai_a380@yahoo.com

***Abstract**: All types of economic institutions have the potential to gather large data volumes related to the activities they are performing. Usually it is possible for the management of such an institution to take advantage of the volume of data that is available and to take informed decisions, based on the knowledge gathered over extended periods of time, instead of taking decisions only by the experience of the management team. In such a way, success on the long term can be attained and the institutions can further improve the quality of their offer to the customers.*
*Decision support data is usually stored in specialized databases or data warehouses that are hosted on specialized servers. These servers must be secured against all types of events that can impede their correct functioning.*
*The present paper is focused on modelling and describing a work frame with the requirements that ensure the security of data used by economic organizations. Among these requirements can be mentioned: the existence of business continuation and disaster recovery plans, the existence of escalation paths for solving problems in a timely manner, preserving the uniformity of data in order to make analysis processes more straightforward, in a shorter period of time.*

**Keywords: data security, data security work frame, decision support.**

## 1. Problems that Can Affect Economic Organizations Data

All kinds of economic institutions have the potential to collect, over time, large amounts of data related to activities carried out by them. Usually, it is possible for the management of such institutions to use the amount of available data for taking informed decisions based on the knowledge accumulated over long periods of time, instead of using only one's personal experience. In this way, long-term success can be achieved and the institutions can improve the quality of their offer to customers [1].
Decision support data is usually stored in specialized databases or data warehouses that are hosted on specialized servers [2]. These servers must be protected against all types of events that can prevent proper operation thereof.
Problems that can affect data owned by economic organizations can have multiple sources, having causes ranging from a local to a global level.
Figure 1 presents the threats faced by companies in relation with their data.
On one side there are the threats coming from the global level and on the other side there are the threats that come from the local level. In this context there can be defined a boundary between the environments from which the two types of threats come:

DOI: 10.1515/kbo-2015-0130

- Inside the defined boundary there is a local environment where things can be more or less controlled and their causes eliminated before they bring serious consequences.
- Outside the defined boundary the causes of the threats cannot be controlled by the economic organization and, as a consequence, these threats have to be faced and overcome.

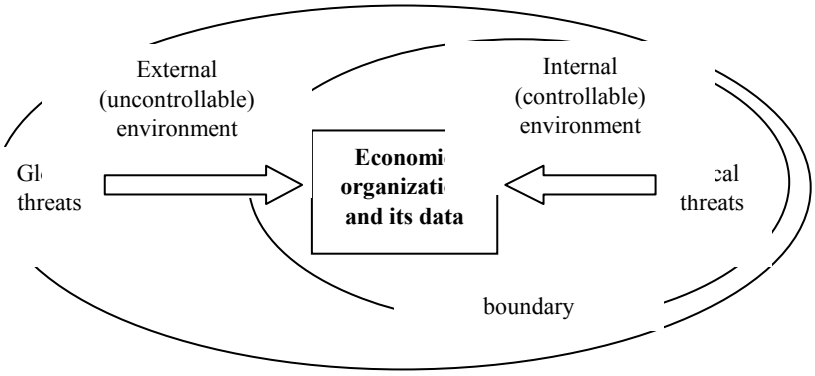


*Figure 1. Threats that can affect a company*

*Threats present at a global level (external threats)*

According to the 2015 Global Risks Report [3], at a global level, there can be identified a number of threats concerning the technological domain which can be relevant to companies that have volumes of data and exploit them by employing business intelligence type tools. The most important issues are presented in Table 1, together with their likelihood and potential impact, represented on a numerical scale

*Table 1*

| ***Possible technological problem*** | ***Likelihood*** | ***Potential impact*** |
|---|---|---|
| *Critical information infrastructure breakdown* | *4.3* | *5.1* |
| *Cyber attacks* | *5.1* | *4.9* |
| *Data fraud or theft* | *5.2* | *4.5* |
| *Misuse of technologies* | *4.3* | *4.4* |

While all the four threats from the previous table can have an indirect impact on a company's evolution, not all of them affect the company in the same way.

From an external point of view one can consider that only data fraud or theft and cyber attacks can affect a company directly. These can be directed towards its data and information system by unfair competitors or other interested parties with the purpose to steal valuable data or impede its operation. The other two threats, critical information infrastructure breakdown and misuse of technologies, can be seen more as internal threats by a company and must be managed accordingly.

A company cannot control the external threats and, in this context, the best policy appears to be preparing to face them, so when they appear, the prejudices caused are reduced to a minimum.

*Threats present at a local level (internal threats)*

Local threats are different from those at global level through the fact that the economic organizations facing them usually have control over their causes.

An example of a local threat could be one's critical information infrastructure breakdown (such as the loss of data resulting from a defect or an undesirable event). This kind of threats can be

prevented by designing information infrastructure with redundancy to ensure data security (duplication of critical resources, ensuring appropriate technical support, performing regular backups etc.).
The best approach for managing local threats is the removal of their causes, most of the times prevention measures being less expensive than facing the threats.
In relation to the data storage methods, there can be identified a number of different problems that can happen to data gathered by economic organizations. Among these the most commonly encountered problems are:

- Loss of data (temporarily or permanently) – loss of data, from the point of view of institutions that are relying on it, means that their operations are impeded, having consequences like inappropriate decisions, reduced efficiency etc. Loss of data can be irreversible or not, depending on the data security measures that are implemented by the data owners. Possible causes of data loss can be: hardware server problems, disasters (fire, theft etc.), software problems, users/ administrators miss operation etc.
- Loss of data access (temporarily or permanently) – loss of data access is different from loss of data, the main difference being that the data is not destroyed, and, at least in theory, it could be accessed again. Most of data access problems are temporary, being caused by events like power supply interruption, network/ internet connection problems etc. The consequences of loosing access to data can be the same as those of loosing data, but are usually less serious than those because in most cases, after the problems are solved, the companies' operations can be carried on normally.
- Unauthorized access to data for other persons or organizations – unauthorized access to data can be very serious and it can potentially be the cause of all the other problems. If unauthorized people have access to data, they can destroy the data or they can alter the data sometimes even without data owners knowing. To these we must add the data theft. Data owned by one company can be used by its competitors to gain advantage on the market.
- Data alteration – data alteration can have serious consequences for a company, resulting in inappropriate decisions, reduced client satisfaction, defective products etc. Data alteration can have a multitude of causes, like human errors, software errors, hardware failure, unauthorized access (outside interference) etc. A company can implement different policies to prevent data alteration.

In the context presented above, Figure 2 summarizes the main problems affecting companies' data together with their causes and consequences. Each company can make a particular schema regarding its problems related to data security in order to track the causes of these problems and find solutions.

**Economic Organizations Data Security Levels**

Data owned by economic organizations has to be stored in a secure way so that the probability of its alteration is as reduced as possible, increasing the organization's ability to take advantage of it.
There can be identified a number of levels at which data security levels must be ensured:

- Physical access security level – it involves controlling unauthorized access to data storage equipment owned by the economic organization; when data is stored in the cloud (storage is outsourced), securing access to data storage devices no longer lies with the economic organization;
- Hardware security level – it involves the use of hardware designed to be resistant to errors / defects (e.g. doubling critical resources to ensure data integrity);
- Software security level – it involves the use of programs that permit access only

to authorized people (e.g. using passwords and other security systems that prevent access to other persons); it is also essential to use software that has data recovery facilities;

Data security level - one can implement a range of optional policies such as the creation of data copies (backups).

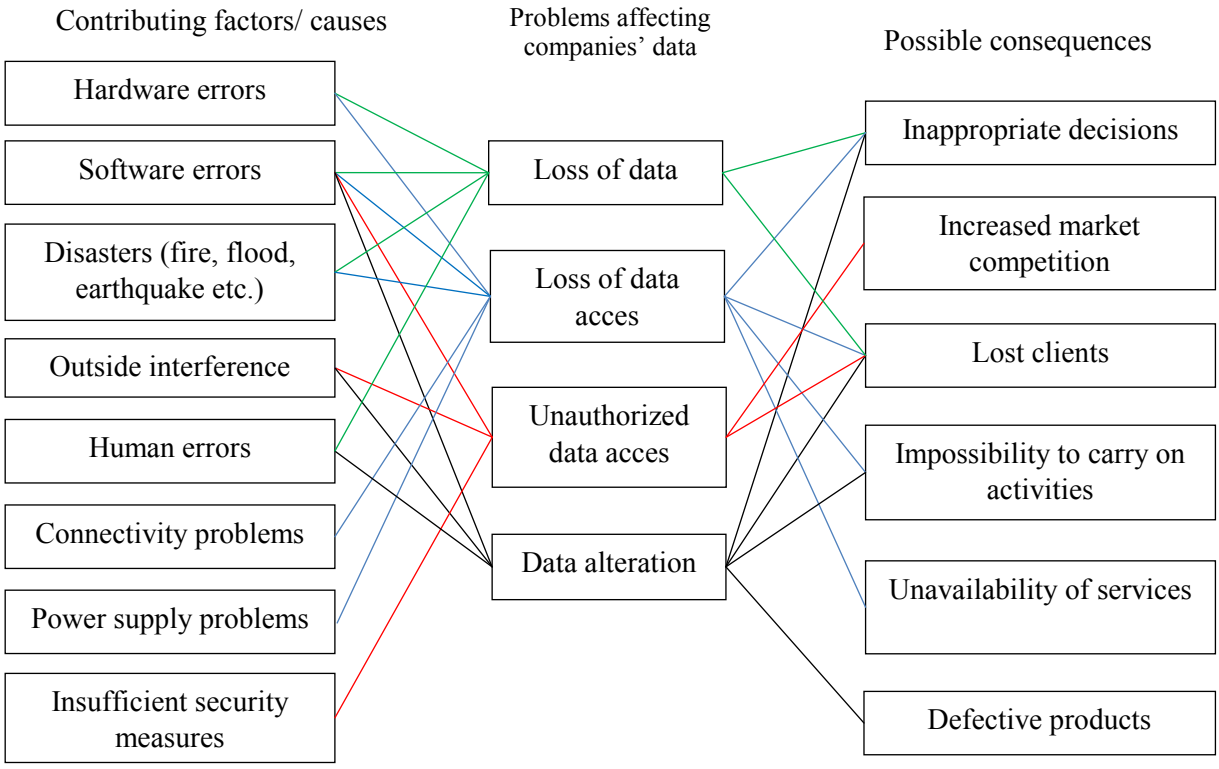


*Figure 2. Problems affecting companies' data, contributing factors and their consequences*

Each of the four levels presented above are detailed in Figure 3.

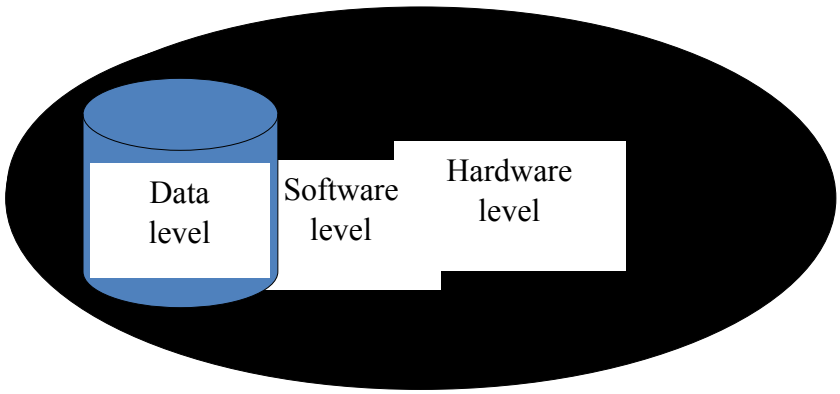


*Figure 3. Data security levels for an economic organization*

**Work Frame for Ensuring Economic Organizations Data Security**

In the context of the vulnerabilities presented in the previous paragraphs, a number of security measures have to be systematized in a coherent work frame that can be implemented by economic organizations that have important volumes

of data be exploited by business intelligence type tools. This work frame has to meet the two previously identified data security requirements:

- Covering all the problems that can affect an organization's economic data;
- Covering all levels at which these issues may arise.

In order to be possible to answer a multitude of problems that may occur on different levels, the proposed work frame will contain solutions structured in an array form. Thus, Table 2 shows a two-dimensional array containing the preventive measures that a company can take to ensure its data security, structured on levels categories of problems.

*Table 2.*

| | ***Physical access security level*** | ***Hardware security level*** | ***Software security level*** | ***Data security level*** |
|---|---|---|---|---|
| ***Loss of data*** | • Keeping servers in secure facilities<br>• Storing copies of data in different locations | • Using reliable equipment to minimize the risk of failure<br>• Having disaster recovery plans | • Using data recovery software to allow for error recovery | • Implementing effective back-up / recovery policies<br>• Existence of escalation paths |
| ***Loss of data access*** | • Ensuring reliable data connections<br>• Redundancy of data connections | • Using reliable networking equipment | • Using special programs to make buffer copies to the most frequently used data | • Keeping copies of data in multiple locations available at anytime<br>• Existence of escalation paths |
| ***Unauthorized access to data for other persons or organizations*** | • Ensuring safety of the data storage location<br>• Installation of alarm systems, burglarproof systems etc. | • Installing critical hardware in an environment where only authorized individuals have access | • Using data encryption software<br>• Using software with special security policies | • Implementing strict security policies<br>• Existence of escalation paths |
| ***Data alteration*** | • Controlling the access to the location where data is stored | • Using reliable hardware to minimize the possibility of data alteration due to errors | • Using software properly tested to ensure data integrity | • Keeping copies of significant data<br>• Business continuation/ recovery plans |

Depending on the importance of the data owned and the costs involved, taking into account the data security measures presented in Table 2, each company can

implement its own informational security policy. The presented array can be customized in order to meet the data security requirements for each economic organization.

The possibility of further developing the proposed array is worth considering as a future direction of research so that it can be applied for a greater number of issues that can affect an organization's economic data.

**Conclusions**

Once with the spread of data analysis systems among businesses, data security problems also emerged.

The threats a business is facing related to one's data can be at a local or a global level, companies having more or less control over the causes of these threats.

In this context, a careful analysis has to be done to calculate the costs of preventing data threats versus facing them, and an informed decision should be adopted by companies.

Because it was found that data security issues are complex, appearing on multiple levels and having different consequences, it was considered necessary to create a work frame that can be used as a guide by economic organizations to better manage their own data risks.

The work frame proposed consists of a two-dimensional array of preventive measures that a company can take to ensure data security levels for different types of problems.

As future research direction, this array can be further extended in order to address other types of problems appearing on different levels.

**Acknowledgements**

This work was financially supported through the project "Routes of academic excellence in doctoral and post-doctoral research - READ" co-financed through the European Social Fund, by Sectoral Operational Programme Human Resources Development 2007-2013, contract no POSDRU/159/1.5/S/137926.

**References**

[1] Miller G., Bräutigam D., Gerlach S., Business Intelligence Competency Centers: A Team Approach to Maximizing Competitive Advantage, John Wiley & Sons, 2006;

[2] http://www.techopedia.com/definition/345/business-intelligence-bi

[3] World Economic Forum, The Global Risks Report, 2015.