Theoretical and Applied Informatics
ISSN 1896–5334
Vol.23 (2011), no. 1
pp. 73–82
DOI: 10.2478/v10179-011-0005-9

The Modeling of Business Impact Analysis for the Loss of Integrity, Confidentiality and Availability in Business Processes and Data

JACEK BAGIŃSKI[a] , MACIEJ ROSTAŃSKI[b]

[a]The Institute of Innovative Technologies EMAG
ul. Leopolda 31, Katowice, Poland
jbaginski@emag.pl

[b]Academy of Business in Dabrowa Górnicza
ul. Cieplaka 1C, Dąbrowa Górnicza, Poland
mrostanski@wsb.edu.pl

Received 25 November 2010, Revised 12 December 2010, Accepted 4 March 2011

Abstract: In this article, authors analyze methods of the analysis of data integrity, security and availability loss results for business processes. Assessing those results, one can judge the importance of a process in organization; thus, determine which business process requires more attention. The importance of those processes can be determined with Business Impact Analysis (BIA). In article, first phase of BIA is presented – in specific, a construction of Business Impact Category Tables, Loss Levels and process weight calculation methods. A variety of weight calculating methods is presented. Authors also present their proposed method – square sum percentage – as a solution eliminating problems of other weight calculation methods in business impact analysis.

Keywords: security, availability, continuity, business impact, risk assessment, BIA

1. Introduction

In this article, authors analyze methods of assessment of data integrity, security and availability loss results for business processes. The presented method is planned to be used for the OSCAD[1] project [1], which assume, among others, integration of two similar management systems in organization: Business Continuity Management System (according to [2]) and Information Security Management System (as stated in [3]).

[1]Full name: Computer Aided Business Continuity Management System – OSCAD (*pol. Komputerowo Wspomagany System Zarządzania Ciągłością Działania) funded by Institute of Innovative Technologies EMAG and Polish Ministry of Science and Higher Education.*

OSCAD will provide a computer support for the organization's business continuity management (including business continuity management of IT infrastructure) and information security management concerning the data processed in the organization and its IT systems. The computer support will cover, among others, such elements as:

- risk management:
  - risk analysis and risk assessment including all possible threats and vulnerabilities (also for IT infrastructure),
  - selection of technical and procedural security measures with respect to the results of the risk (levels) analysis,
  - reports preparation,
- incidents management:
  - incident data acquisition (manual acquisition – from the users, and automatic acquisition – from electronic sensors),
  - incident handling (loss of business continuity, loss of data security – confidentiality, integrity, availability),
  - generating reports and preparing statistical data about incidents,
  - audits management (e.g. audits which check compliance with information security standards, quality standards, etc.),
  - maintenance of a central database with threats, vulnerabilities, security measures applied by the organization and recorded incidents,
  - collecting data about incidents and providing access to statistics about incidents.

The risk analysis method described in the article was implemented in a module which analyzes and assesses the risk level for the data processed in the organization and for the processes which take place there. The module provides a report with a list of security measures which either were implemented or are to be implemented in the organization and its systems. These measures are to ensure that the systems and processes of the organization function on a required level of reliability and that the information is processed on a proper (assumed) security level.

In every organization one can define business processes – as thoroughly described for example in [4] or [5]. In fact, the outcome of wide implementing of ERP systems is that enterprises have to carefully design and monitor their business processes. Each organization is aware of the key processes and sub-processes; some are core processes (critical to operation), some may be supporting (important, yet secondary).

The importance of those processes can be defined with Business Impact Analysis (BIA). BIA is required, among others, by BS 25999 norm [2]. It also may be a part of risk analysis process in an Information Security Management Systems implemented in accordance with ISO 27001. The main concept is to provide a method for assessment of loss value in case of: (1) a breach of confidentiality of processed data, (2) a loss of data integrity or process activities integrity, (3) a low process availability (operation breaks or lack of incoming information). Such analysis may be performed during assessment workshops involving the process owner and representatives of enterprise organizational units, engaged in business process realization. The proposed method is, in fact, combination of several other methods described in [6] and also was patterned on the method described in [7].

BIA is the basis method which assume security attributes loss assessment. The assessment is performed with surveys fulfilled during interview and workshops with personnel responsible for the process. The attribute loss assessment may be performed with Structured What-if method usage. Survey may contain questions 'what would happen, if...', which refer to set of possible impacts. Such survey will also help to stimulate the discussion as well as threats and vulnerabilities identification.

The loss level may be assessed using tables, such as Likelihood definitions or Magnitude of Impact definition tables (described in [7]), or just like in Consequence likelihood matrix method (presented in [6]).

Any further analysis is performed (in the first place) for the processes with highest loss level assessed, which means the highest value (importance) for organization. The risk level for identified threats and vulnerabilities may be assessed e.g. with the Likelihood criteria matrix [6] or with the Risk-level matrix [7] usage. In case of OSCAD Project, the risk level assessment is performed by inserting to the formula such values like the assessed process value, threat probability, vulnerability and controls implementation level.

Based on such analysis results, one can define the importance (weight) of specific process, and select key processes intended for special treatment – more detailed risk analysis. Authors present example methods of such weight calculation and propose theirs.

2. Business Impact Category Tables

In the first phase of BIA, for every attribute (confidentiality / integrity / availability) the analysis is based on specific Business Impact Category (BIC) Tables. BIC Table consists of impact categories (rows), and for each one of them loss level is assigned. For different impacts, loss level (weight) may be different, and it may vary for every attribute (confidentiality / integrity/ availability). Results for every table row (impact

category) should assemble to overall loss values, hence – the importance, for given business process at given attribute.

2.1. Business Impact Categories

The BIC Table requires defining N specific impact categories. Such categories may vary for every enterprise and may require refining or adjusting, but categories proposed in this article seem adequate for majority of organizations. In this case, N = 4. Those are:

1. Human (Personnel/Client) related losses,
2. Law violation,
3. Financial losses,
4. Effectiveness drop (Lowered quality, production losses, delayed realization).

2.2. Loss levels

For convenience, the loss levels may be identified using descriptive notes, for example using loss matrix (patterned on *Magnitude of impact definitions* – [7]), defined locally inside organization. But for the purpose of mathematical methods in next steps, those descriptions should be assigned to numerical values. Assuming every enterprise is able to create own scale of loss levels, one can define that every organization for every N categories for every attribute analysis assigns level j, where:

$$j \in N, \quad 1 \leq j \leq n, \tag{1}$$

And n value is maximum loss level (in reality, rarely more than 5).

Interpretation of numerical and descriptive loss levels concept is shown on Table 1.

Loss level	**Matching value and description**
Lowest	**1** No or insignificant losses in case of confidentiality, integrity or availability incident; Confidentiality example: data publicly available
	...
	...
Highest	**n** Major losses, threat to further organization functioning Confidentiality example: Top secret data requiring maximum security

Tab 1. Numerical and descriptive loss levels table

Mapping loss levels table onto Business Impact Categories should be adjusted and adapted within specific organization needs and environment. This process is a difficult part of the analysis, as descriptions of losses and their consequences may be very specific

to given organization; therefore, well chosen descriptive values provide help during assessment phase and constructing BIC definitions with organization representatives. Such definition example is shown on Table 2. In this example, n =3. Descriptions defined in loss level table in earlier phase are greyed out.

BICs	Loss level
	1 – No significant damage *2 – Attribute breach may cause significant damage, recoverable with mediocre financial expenditures* *3 – Possible major damage, threat to business continuity. Possible damages to client, partner or supplier.*
Human (personnel/clients) related losses	1 – No effect on personnel/clients 2 – Possibilities of injuries 3 – May cause human death or serious injury
Law violation	1 – No infringement 2 – Organization may have limited possibilities of activity caused by lawsuits 3 – May be a cause to stop all institution activity
Financial Losses	1 – Up to 50 000$ 2 – Up to 500 000$ 3 – Over 500 000$
Effectiveness drop	1 – No difficulties 2 – Break in process continuity for couple of hours 3 – No further service possible

Tab 2. Loss level definition table example

2.3. BIC table example

Given loss levels description table, one is able to construct BIC Table. Proposal of such BIC Table for confidentiality / integrity loss is presented in Table 3.

During a workshop, performing BIC Table analysis is difficult to begin with; best case scenario is to start with sub-processes analysis – the representatives of given organization should operate on sub-process level more effectively.

3. Process importance (weight)

After determining all of BIC Table and corresponding loss levels in every attribute (confidentiality (C), integrity (I) and availability (A) areas), an overall weight of the process can be computed. One may choose from many methods used for such calculations.

Basic categories	**Loss level and justification** for each of security parameter		
	Confidentiality	**Integrity**	**Availability**
Human (personnel/clients) related losses	1 Loss of confidentiality has no impact on human life and health	2 Loss of production process integrity may has some influence on personnel health.	2 Loss of production process availability may has some influence on personnel health.
Law violation Is data confidentiality/integrity/availability required by law In this process? May data confidentiality/integrity/availability loss result with law violation?	3 Personal data confidentiality is required by law. Loss of confidentiality may block the realization of the process because of impose sanctions by the regulator.	2 Data integrity is required by bilateral agreements. Loss of integrity may results of lawsuit.	2 Data availability is required by bilateral agreements. Loss of availability may results of lawsuit.
Financial losses Costs of data/process/service/system recovery, cost of client damages,fines?	2 Financial penalties due to confidentiality breach.	2 Data integrity may results of financial loss due to claiming damages.	2 Data availability may results of financial loss due to claiming damages.
Effectiveness drop Is the data, which confidentiality is important for realized activities, used in the process?	1 No significant effectiveness drop resulting from data confidentiality loss.	2 Loss of production data integrity may lead to delay of the process realization (restoration of data needed)	2 Loss of the data availability lead to the process effectiveness drop
Overall Overall score can be computed using many methods, for example choosing the most damaging scenario.	3 Disclosure of private client data may affect the regulator's sanctions lead to an end of organization.	2 Loss of process/data integrity lead to losses on a medium level for all impact categories.	2 Loss of process/data availability lead to losses on a medium level for all impact categories.

Tab 3. Business Impact Category Table example for data confidentiality/integrity/availability loss

3.1. "Worst case scenario" method

Overall process weight is determined as the highest loss value in any attribute and category. This simplest method has one flaw – most of key processes most likely are going to have at least one loss level at the highest value (n), leading to the impossibility of process weight comparison.

3.2. Arithmetical sum of loss levels

Calculating a sum of all loss levels at C, I, A attribute is a crude, but effective method of calculating weight. This however may result in an unbiased weight. Let's consider an example of two processes P_i with S_i solutions and weights W_i below, where n=4 and N=4.

$$\begin{array}{ll} S_1(P_1) = (4,4,1,1) & W_1 = 10 \\ S_2(P_2) = (3,3,2,2) & W_2 = 10 \end{array} \tag{2}$$

The process P_1 has two maximum loss levels (losses are catastrophic), so it should be more important than P_2. This situation is often met at real environment and both methods, *worst case scenario* and *arithmetical sum* fail to recognize the situation. Moreover, any comparison between two BIAs (which may be necessary for example if two organizations merge) is impossible if N and n values differ in those analysis.

3.3. Process weight matrix

The importance (weight) of the process can be determined using Process Weight Matrix, a concept eliminating flaws of above methods. Simply put, process weight matrix is a table, where all possible combinations are assigned to specific weight as an outcome of organization representatives' decision during business impact analysis and assessment.

Given following BIA parameters: N=3, n=3, an example of process weight matrix is presented in Table 4.

Solutions vector S	Process weight
– (3, 3, n) n=2..3 – (3, n, 3) n=2..3 – (n, 3, 3) n=2..3	4
– (3, n, n) n= 1..2 – (n, 3, n) n= 1..2 – (n, n, 3) n= 1..2	3
– (2, 2, n) n= 1..2 – (2, n, 2) n= 1..2 – (n, 2, 2) n= 1..2	2
All other cases	1

Tab 4. Process weight matrix example

Problem of this method is that construction of the matrix is time-taking and every new organization analysis requires a new matrix. Another major flaw of above methods is lack of scalability and comparison ability. To interpret weight value, loss level scale (n value) has to be known for the process.

3.4. Square sum percentage

A method proposed by the authors eliminates described problems. Also, normalization for scalability and comparison purposes is introduced.

Overall value W for process weight is calculated as percentage of sum of squares of loss values for every impact category S_i, in sum of squares of maximum loss values, which can be defined as:

$$W = \frac{\sum S_i^2}{N_k \cdot n^2} \cdot 100\% \quad , \tag{3}$$

where S_i means loss levels for every category in BIC Table (solutions in S vector).

Referring to the example described in 3.2, two processes weights are calculated as follows:

$$\begin{array}{ll} S_1(P_1) = (4,4,1,1) & W_1 = 53,1\% \\ S_2(P_2) = (3,3,2,2) & W_2 = 40,6\% \end{array} \tag{4}$$

As stated, contrary to *arithmetical sum* and *worst case scenario* methods, two processes have different weights, and higher loss levels cause weight W_1 to be stronger as expected.

4. Conclusion

The modeling of data integrity, security and availability loss results for business processes may start with Business Impact Analysis. In this analysis, one has to determine specific to organization Business Impact Categories, which combined with Loss Levels Definition, lead to Business Impact Categories (BIC) Tables design – a concept of assigning a loss levels table to Business Impact Categories for data security attributes loss: confidentiality (C), Integrity (I), Avalability (A).

Given the Business Impact Categories Tables for every attribute loss in a business process, one can calculate the importance of a process in organization; thus, determine which business process requires more attention.

This article presents a variety of importance determining methods by calculating process weight values. Authors present their proposed method – square sum percentage – as a solution eliminating problems of other weight calculation methods in business impact analysis.

References

1. A. Białas: *Komputerowo wspomagany system zarządzania ciągłością działania – założenia projektu, Materiały konferencyjne EMTECH'2010 – Zasilanie, informatyka techniczna i automatyka w przemyśle wydobywczym – Innowacyjność i bezpieczeństwo*. Ustroń, 19-21 maja 2010, pp. 29-37.
2. BS 25999-2:2007 *Business continuity management – Part 2: Specification*.
3. ISO/IEC 27001:2005 (formerly BS 7799-2:2002) *Information Security Management System*.
4. H. J. Johansson et al.: *Business Process Reengineering: BreakPoint Strategies for Market Dominance*. John Wiley & Sons, 1993.
5. T. Davenport: *Process Innovation: Reengineering work through information technology*. Harvard Business School Press, Boston 1993.
6. IEC/FDIS 31010:2009 (Final draft) *Risk management – Risk assessment techniques*.
7. G. Stoneburner, A. Goguen, A. Feringa: *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30. Gaithersburg, MD, U.S., 2002.
8. T. P. Layton: Information Security: *Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach publications, 2007.
9. J. W. Rittinghouse, J. F. Ransome: *Business continuity and disaster recovery for infosec managers*. Elsevier Digital Press, 2005.

Modelowanie skutków biznesowych dla utraty poufności, integralności i dostępności danych i procesów biznesowych

Streszczenie

Realizowany przez Instytut Technik Innowacyjnych EMAG system OSCAD (Otwarty Szkieletowy System Zarządzania Ciągłością Działania) ma realizować komputerowe wspomaganie zarządzania ciągłością działania organizacji (w tym również zarządzanie ciągłością działania infrastruktury IT) oraz zarządzanie bezpieczeństwem informacji przetwarzanych w instytucji, jej systemach informatycznych. Komputerowe wspomaganie będzie obejmowało m.in. takie elementy, jak zarządzanie ryzykiem oraz zarządzanie incydentami.

Opisywana w artykule metoda analizy ryzyka została zaimplementowana w module służącym do analizy i oceny poziomu ryzyka dla danych przetwarzanych w organizacji oraz realizowanych procesów. Wynikiem działania tego modułu jest następnie raport z listą zabezpieczeń wdrożonych oraz wymaganych do wdrożenia w organizacji

i jej systemach w celu zapewnienia wymaganego poziomu niezawodności funkcjonowania jej systemów, procesów oraz zapewnienia właściwego (założonego) poziomu bezpieczeństwa przetwarzanych informacji.

Autorzy analizują sposób modelowania skutków biznesowych dla utraty poufności, integralności i dostępności danych i procesów biznesowych. Zaprezentowano pierwszą fazę BIA (analizy skutków biznesowych), a zwłaszcza konstrukcję tabeli kategorii skutków biznesowych. Przedstawiono różne metody kalkulacji wagi (znaczenia) procesu dla organizacji. Autorzy proponują własną metodę – procenta sumy kwadratowej – jako rozwiązania eliminującego problemy innych metod kalkulacji wagi procesu w analizie skutków biznesowych.