BUSINESS PROCESS MANAGEMENT, AN IMPORTANT AID IN OPTIMIZING ORGANIZATIONAL PROCESSES IN NATIONAL SECURITY INSTITUTIONS

Laurentiu Barcan, PhD

University of Craiova, Craiova, Romania

Being required to conform to the large number of regulations, standards and requirements, information security should be considered a general problem of organization that requires involvement at the level of management and must involve all departments and activities of an organization, from professionals in the field to information to users. Creating a culture of security is essential to the organization through continuous education of staff, permanent collaboration with partners in a common approach to security issues, but also through customer awareness of information security risks.

Key words: Business Process Management, Business Process Execution Language, Intelligent information systems, National security

1. INTRODUCTION

Romania is becoming more attractive to hackers and Internet fraud seem not to stop anyone bypass. Last year, Romania has experienced forty two millions computer security incidents and were affected approximately two millions IP address. Most have focused on financial and banking system, public institutions and NGOs. Operational risk, the novelty brought by Basel II, is the risk of direct and indirect losses caused by internal factors and external factors.

Securing organizational processes is an objective and a permanent objective of organizations active in the field of national security, for this there are different solutions, both software and hardware. A modern solution may be the efficient use of Business Process Management (BPM) and Business Process Execution Language (BPEL) as tools to optimize and streamline the decision flows.

Operational risk is the most controversial, the least defined and most likely will have a major evolution in the coming years. The impact of operational risk can affect relationships with customers and partners, and its implications values are difficult to measure accurately. The technological revolution has led to a reassessment of human perception of the surrounding world and the explosion of information technology has increased the number of communication methods between individuals.

2. NATIONAL SECURITY AND CYBER ATTACKS

Using computer systems through their applications in operational, managerial and create a competitive advantage ensures the organization of local, national (in collaboration between departments, between hierarchical levels) to form the exchange of information using the Internet. For this purpose, the basic concepts of intelligent information system provide technical and behavioral elements that help substantiate specialized applications, the decision-making process and to build a strategic advantage against competitors of the organization.

Business processes can be described as executable business processes, which shape current behavior of a participant in a business interaction protocols and the business processes that use descriptions specifying the behavior of parties to exchange messages without discovering their internal behavior. Access to information and rapid transmission from one continent to another, and still have

both positive and negative consequences on the development of moral, psychological and social development of individuals, on the structure and functioning of society in general.

Many network security attacks come from within. Internal attacks refers to theft of passwords (which can be used or sold), industrial espionage, disgruntled employees who tend to cause damage to the employer, or simply misuse. Most of these violations can be resolved by using corporate security officer who monitors the network users. Among the internal factors that influence operational risk we can include: conducting inefficient internal processes, inadequate staff training, quality systems used.

Information security issues also come into the category of factors that have direct implications on operational risk: partial or complete systems falling out, problems caused by attacks or intrusion, fraud, operating errors, off work for a certain period, and more. Corresponding operational continuity planning, policies, standards and procedures to ensure timely maintenance and resumption of operations in the event of interruptions help reduce risks and add value to the organization.

The relationship between Internet and globalization can be seen as a relationship in which each factor influences the other. Globalization is a phenomenon tends to emphasize extensive and ever more. Today most large organizations have developed systems globally as a consequence of the difference in costs in various places around the globe, while pointing out the existence of small and medium-sized organizations the use of the Internet becomes a primary mean of communication for their activity, an important mean of promotion.

Network security is now an integral part of computer networks and it involves protocols, technologies, systems, tools and techniques to secure, and stop malicious attacks. Cyber attacks have increased significantly in recent years and according to Europol reports, crimes committed in cyberspace causes annual losses of over one trillion USD. Romanian Intelligence Service will launch early next year a program worth ninety seven million euros with which to protect at least state institutions cyber attacks. The money comes from European funds. In addition, companies that invest in cyber security could benefit from tax incentives.

3. CYBER WORLD AND NATIONAL SECURITY

Computer security is a branch of computer science (computer science) that deals with identifying risks involved in the use of computers and their removal solutions. Information security is concerned with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The three components of information security are confidentiality, integrity and availability. Confidentiality is ensured by encrypting information. Integrity is obtained by dispersing mechanisms and algorithms. Availability is ensured by strengthening network security systems or networks and providing backup.

With the increasing number of digital payments, grow also the security issues. For this reason, you should increase the importance of information security related education both in schools and in the management of state institutions and private banking, who do not understand how cyber attacks can be dangerous, especially since many institutions have sensitive data that may reach the wrong hands.

Cyber security has become one of the major components of the Internet. Analysts have noticed a contradiction between the need for communication and connectivity, on the one hand, and the need to ensure confidentiality, integrity and authenticity of data, on the other hand. The relatively new field of information security seeks technical solutions to resolve this apparent contradiction.

The speed and efficiency of communications and documents instant messaging gives many pluses of decision-making in a modern society based on competitive economy. But using email

services, web, transfer funds, etc. is based on a feeling, often fake security communications that can transform potential earnings, such as rapid access to information in major losses caused by data theft.

Information security requirements grow in the context of credit institutions to connect the infrastructure payment, settlement, and reporting system established at national, regional or global level. The need to ensure security at the system level translates into minimum security requirements for each participant, a participant's security problems can affect the functioning of the entire system.

Business Process Management is focused on managing change and improves business processes. Business Process Management unites different disciplines: previous process modeling, simulation, workflow, Enterprise Application Integration (EAI) and Business-to-Business Integration (B2B) in one standard. The fact that Business Process Management is a new initiative can make you believe that business processes were not previously managed. This of course is not true - many organizations have shaped and manage their business processes over the years using a wide variety of techniques and tools.

These techniques have been successful partly or totally failed because it was a lack of standards and a full life cycle to control and guide the design and execution of business processes. Managing the change process can not be an ad hoc process - it is necessary to control management on innovation, architecture, design and processes. For site management to understand the architecture, design and deployment processes requires modeling standards in business and execution of business processes.

4. BUSINESS PROCESS MANAGEMENT IN NATIONAL SECURITY

Business Process Management is a structured software solution with role modeling and optimization of current activities (especially repetitive) of an organization and human interactions inside and outside them, operating with them in the form of processes. Information systems in the field of national security organizations have a high level of heterogeneity, but BPM provides solutions for integrating highly diverse systems.

The business consists of any group of activities carried out in order to produce a particular result or to specific customer oriented market. This result appears as a consequence of globalization. In a modern organization, information technology is leading to new guidelines that require the use of increasingly sophisticated means (artificial intelligence, expert systems, etc.). The business environment is constantly changing and requires new techniques and methods of preparation of the process.

Unlike traditional systems, Business Process Management offers advanced features for modeling and automating business flows in the organization. Also, access to diverse data sources is much easier, due to a large number of applications interoperability. New technologies based on BPM enable business processes that can be modeled directly by analysts (operative, financial and economic), without the support of IT departments.

Technologies and standards used in implementing BPM are XML and Web services. The latter represents a standardized way of communication between Web applications. The language, specific to BPM, is Business Process Execution Language. It is defined by a standard based on XML and Web services, which allows modeling and automating their business flows. With this dedicated language, business flows and business rules can be defined in an intuitive way. Thus, there is provided a high level of transparency in making business operations. Thanks to these innovations, BPEL technology simplifies the integration of various applications and business processes.

Business Process Management solutions are used both to automate internal processes within the organization and with partners to conduct flow. These solutions offer flexibility in integrating and automating complex business processes, involving several organizations. The implementation of BPM technology in existing computer systems

requires a complex information analysis. This identifies business processes and establishes correlations between them.

Switching to new technology can not be made without a cost analysis. This analysis will seek to identify the size of the cost of design, implementation and maintenance for various solutions on the market. After the analysis phase, the conclusions will proceed to the construction of management models. This is done using visual tools included in the Business Process Management applications. In fact, they are modeling business processes for their integration with the information systems within the organization.

The instruments used are based on technology UML (Unified Modeling Language) and Business Process Execution Language. As a result, implementation of the solution will be followed by generation of components from models. Testing and optimization of the solution is the last stage of implementing BPM. It involves testing the menus business processes, correction of programming errors or modeling, and optimization of these processes.

BPEL is an XML-based language. It allows developers to describe their business processes as Web services. Language is derived from languages WSFL (Web Services Flow Language) and WSDL (Web Services Description Language), applied to business. BPEL language focuses on modern business process modeling, adopting Web services as external communication mechanisms. It integrates features Web Services Description Language (WSDL) to describe incoming or outgoing messages.

The descriptions of processes in business protocols are called abstract processes. BPEL is used to model processes both executable and abstract ones. For large-scale programming, BPEL language describes the abstract processes as a series of observable behaviors. Thus, it shows you that you have expected / sent messages when you have found compensation for failed transactions etc.

The main role of BPEL in data exchange via Web services is to define all steps in a transaction. The use of BPEL is designed to ensure that they are executed in the correct order. BPEL can automate the sequencing of messages, but does not deal with the effective execution of transactions. Thus, BPEL provides a much cheaper method than stronger (and more difficult) EDI (Electronic Data Interchange).

5. STANDARDS, LAWS, REGULATIONS AND CYBER SECURITY

Business Process Modeling Notation (BMPN) is the new standard for the flow of business processes and web services. Created by the Business Process Management Initiative (BPMI), the main goal of BPMN is to provide a notation that is readily understandable by all users of software for business. This includes people from the business analysts that create the initial projects to technical developers responsible for implementing the technology that will perform these processes.

A second purpose is equally important to ensure that XML languages designed for implementation of business processes such as BPEL4WS (Business Process Execution Language for Web Services) or BPML (Business Process Modeling Language) can be expressed visually by a common notation. BPMN allows business process management (BPM - Business Process Management). Thus, BPMN is a central factor for a new initiative in the world of Enterprise Architecture - Business Process Management.

The lack of a systemic approach increases the capital required for the functioning of financial and banking institutions. To reduce it, according to Basel III, operational risk should be kept in check. Performance indicators should be collected and reported on a concept and a well-developed system. Leaks, even theft determine the need to actively prevent data loss.

Computer applications require active monitoring systems, availability must be real and carefully managed, and abnormal behavior is detected by the computer. User activity must be performed and recorded. IT and information security processes must be based

on clear standards for type ITIL, ISO 27000 standard reporting systems COBIT, and these standards should be reflected in national regulations, in a complete and integrated financial sector specific.

Credit institutions shall respect the laws, rules and regulations containing provisions on information security. Regulatory banking system is contained in the Banking Law and the rules NBR, and Rule 16/2004 on techniques for guaranteeing the authenticity of the signature, and Rule 17/2003 for the organization and internal control of the business of credit institutions and significant risk management. In the field of electronic payments, the most important regulations are MCTI Order 218 / 14.06.2004 and NBR Regulation 6/2006 concerning transactions by electronic payment instruments and relationships between participants.

Other regulations refers to electronic signature (electronic signature Law 455/2001, Law 451/2004 on temporal) and electronic commerce (Law no. 365/2002, as amended by Law no. 121/2006). We have legislation on preventing and combating cyber crime, Law no. 161 / 19.04.2003. A separate chapter is the law on privacy: Law 677/2001 on the protection of individuals with regard to the processing of personal data and Law 506/2004 regarding the processing of personal data and privacy in the electronic communications sector. To this, add a significant number of European Directives in the field of information security. Regulations only partially covers the spectrum of problems they raise: information security, information technology control, risk management and quality services.

Last but not least, with the accession to the European Union, credit institutions may have access to regional infrastructure such payments TARGET2, TARGET2 Securities, EBA Clearing systems (EURO1, STEP1, STEP2) or other payments infrastructure which impose specific security requirements. Also in the Euro Zone, the SEPA project of the Single Euro Payments involves standardizing payment instruments in Euro and new requirements for infrastructure and payment with cards, including a strategy to prevent fraud with cards, by migrating throughout the Euro EMV and implement 3DSecure.

6. MONEY LAUNDERING, A PERSISTENT MATTER IN BANKING

Money laundering is the process or complex actions when criminals sometimes are trying and failing to hide the origin and possession of real income from their illegal activities. This category includes money from fraud, robbery, theft, weapons smuggling, drug trafficking and smuggling. Criminals will try to use the banking system to hide the criminal origin of the money.

The bank prevents money laundering and terrorist financing, following within BPM the rules, procedures and related laws. Under EU law, the bank must have a good knowledge of the business and how they use bank services and products. This means that in some cases, to ensure total transparency and in order to comply with current regulations, the bank will require customer’s information on their activities. Money Laundering Law requires banks to have a good knowledge of their customers' businesses.

Money laundering is the de facto financial crimes which all bring profit. It is the process by which criminals attempt to conceal the origin and actual possession of the income from their criminal activities. Therefore, more and more banking institutions in Romania are recognizing the international standards are the basis of organizing activities and information security.

Also, banks are required to understand the purpose of business relationships and transactions of clients. For this reason, the bank can require certain information to be always treated with the utmost confidentiality, subject to banking secrecy and confidentiality law and protection of personal data.

7. CONCLUSIONS

Information systems are under threat from both inside and outside. They may be well intended people who make different operating errors or malicious individuals who sacrifice

time and money to penetrate computer systems. Among the factors that allow cracks security techniques may be some errors of software processing or communication or computing defective equipment or communication lines. The lack of an adequate training manager, operators and users of systems increases the likelihood of security breaches. Misuse of systems (hacking) is also one of the major risk factors of security systems.

Implementing new technologies in intelligent information systems belonging to organizations working in the national security is welcomed, organizations from the member states organizations in our country are already having these technologies widely implemented. Given the specific processes of change in all these organizations, the current geo-political context, securing business processes through intelligent applications is mandatory, as a primary defense operations and secret documents.

REFERENCES

[1] Barcan, L., Impact of information technology on the implementation of change management in banking, Young Economists Journal, Nr. 19, Craiova, 2012

[2] Barcan, L., Managementul schimbării în securitatea naţională, Editura Sitech, Craiova, 2013

[3] Barcan, L., New issues of organizational processes security in Romanian commercial banks, Young Economists Journal, Nr. 23, Craiova, 2014

[4] Barcan, L., The intelligent information systems, an important aid in national security, Journal of Defense Resources Management, Braşov, 2014

[5] Hontanon, R. J., Securitatea rețelelor, Editura Teora, Bucureşti, 2003

[6] Mihai, I. C., Securitatea informațiilor, Editura Sitech, Craiova, 2012

[7] Ould, M. A., Business Process Management: A Rigorous Approach, British Computer Society, 2005

[8] Weske, M., Business Process Management - Concepts, Languages, Architectures, Springer-Verlag, Berlin Heidelberg, 2007

[9] ***, ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

[10] http://www.biblioteca-digitala.ase.ro/biblioteca/carte2.asp?id=225&idb=

[11] http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-fraudelor-privind-mijloacele-de-plata-electronica/

[12] http://profs.info.uaic.ro/~mihaela/teach/biz/curs09biz.pdf

[13] http://stiri.tvr.ro/conturile-noastre-bancare---in-pericol--sistemul-bancar-este-cel-mai-vizat-de-fraude-informatice_52011.html