DE GRUYTER OPEN
REBS Review of Economic & Business Studies
Volume 9, Issue 1, pp. 157-169, 2016
ISSN-1843-763X
DOI 10.1515/rebs-2016-0030

BUSINESS INTELLIGENCE SECURITY

Dragoş Ovidiu TOFAN*

Abstract: *Excess information characteristic to the current environment leads to the need for a change of the organizations' perspective and strategy not only through the raw data processing, but also in terms of existing applications generating new information. The overwhelming evolution of digital technologies and web changes led to the adoption of new and adapted internal policies and the emergence of regulations at level of governments or different social organisms. Information security risks arising from the current dynamics demand fast solutions linked to hardware, software and also to education of human resources. Business Intelligence (BI) solutions have their specific evolution in order to bring their contribution to ensure the protection of data through specific components (Big Data, cloud, analytics). The current trend of development of BI applications on mobile devices brings with it a number of shortcomings related to information security and require additional protective measure regarding flows, specific processing and data storage.*
Keywords: *Business Intelligence, information control, cloud computing*

1. INTRODUCTION

Business Intelligence tools play a decisive role in the implementation and compliance of management strategies. As a basic definition, Business Intelligence is a set of economic applications designed to analyze data in order to be converted into information that provides consistency to the decision [2].

The multitude of data or information faced by an organization under today's business environment complicate the analysis and control systems. The development of the Internet economy, digitization of most of the processes, considerable cheapening of data sources and access to information, diversity of

* Dragos Ovidiu TOFAN, "Alexandru Ioan Cuza" University, Faculty of Economics and Business Administration, Doctoral School Of Economics and Business Administration, Iasi, Romania, dragos.tofan.2014@gmail.com

knowledge presentation formats led to "bombing" the entities with data/information excess.

The information is considered a good or asset, but only recently organizations have understood its true potential. As its value increases, more attention is given to information management, storage practices, transfer methodologies, disaster recovery and security [3]. This is why focus is on accuracy, consistency and reliability of data to support sound decisions, thus bringing into question the need for integrity of accessible and used information. If, traditionally, information security relies on IT departments within the entities, increasingly more researchers discovered that all employees must be fully involved in this. The Business Intelligence systems must have the ability to help organizations create a culture of information security through monitoring activities, setting goals for users, providing responsibilities [5].

This paper focuses on the information security for BI users because these facilities tend to become essential tools for management in its struggle in a dynamic and competitive market. The main objective is to analyse the best way to reach a desired level of information security, when using BI instruments. In order to bring arguments, the author suggests a number of secondary endpoints:

- Reveal context – a short introduction in the world of big data and cloud computing
- The notion of information security – definition and trends in the BI environment
- Approaches on improving information security – threats, costs and benefits.

A case study is shortly analysed in order to underline the role of Business Intelligence in improving efficiency in terms of financial results and also in terms of acquiring a higher security level in the information flow.

2. CONTEXT – BIG DATA, CLOUD, ANALYTICS

Storage facilities automatically refer to the concept of data warehouse that are providing architectures and useful tools for the executive management, through systematic organization, understanding and use of data in making strategic decisions [1]. Building and maintaining a successful trustworthy data warehouse

became the result of a joint composed of an automated control of information, partnerships and execution [3].

Data storage has always been a vital item for BI capabilities as technology is dynamic and a constantly changing one. Due to the opportunity of storing information at low costs, BI manager goal is somehow to filter and manipulate this asset of the company for the construction of accurate predictive models [4].

Invariably there must be taken into consideration the term of Big Data which can be defined as a set of techniques and technologies that require new forms of integration to discover the value in a data set characterized by diversity, complexity, and at a massive scale. Thus, the information acquires a new dimension and it increases in value based on robust and adjustable analytics platform. In the 2001 research report, META Group (now Gartner) defines Big Data through the prism of 3 elements (the 3 V):

- **Velocity** - data are processed at a high speed. Although real-time processing brings benefits, it puts pressure on the ability to validate data and the entity infrastructure.
- **Volume** - information captured through various channels by consumers is of huge volume, making data traditional sampling almost impossible. In terms of internal policies and authorization levels, the question of data storage exists within the entity.
- **Variability** - data aggregation becomes a challenge as big data involves unstructured and different formats: text, image, audio, video, etc. and missing parts are replaced by merging data.

  In 2012, Gartner updated the definition by introducing the fourth V:
- **Veracity** - this new coordinated highlighted in the representation of Big Data is oftenly forgotten, although it is essential for a successful business.

Under the current conditions, the growing complexity of information flow facing any organization suggest the idea of pressure from speed, volume, and variability factors on veracity of big data. But these dimensions must work together and provide value through specific technologies and analytical methods. Thus, the emphasis is not only on the processing capacity but also the accuracy of the data processed.

The huge volume of data which needs to be processed through existing facilities and the need for quick access to the terminals in common use has led to the solution of Cloud Computing. The benefits derived from cloud storage

availability on multiple devices with increased mobility give the companies the opportunity to escape from investments in software, hardware and storage infrastructure required for operations and data analysis. The applications and data are running and stored somewhere other than on the user's servers and terminals and the access is done from distance. Thus, it becomes more attractive to buy Business Intelligence resources that folds domestic demand from option of building and maintaining its own data warehouse.

Ironically, this variant of storage created serious enough security risks for a business through the proposed centralized BI architecture. It can be said that many potentially sensitive data are gathered in one place and accessed by many users. Gaining access by an attacker may lead to theft or damage of data in large quantities. Moreover, cloud storage does not maintain or drive itself. This kind of storage is, after all, a business requiring administrators and managers who understand the internal software and the security issues in the cloud.

3. INFORMATION SECURITY

As a simplistic definition, information security can be seen as a protection of integrity, availability and confidentiality of data and systems, which is vital in maintaining the operations of an organization [5]. Oftenly, this concept can be seen as software and hardware systems designed to improve information security. There are examples of well-known technologies like anti-virus programs, firewalls, anti-spyware, based on technology that alerts and tend to frustrate users who ignore and even close these protective systems in many cases.

Hence, it becomes essential to have an analysis of the causes of security issues in the sense that these cannot be left solely to the discretion of the IT departments, but requires an approach through the prism of business and through the human factor. From the business point of view, management is interested in how the information security protects the organization. The budget allocated influences the level of security that an entity can maintain. Thus, a risk analysis and an estimation of cost in case a security breach, unfortunately, drive often to the conclusion that undesirable expenses should be budgeted, and this should be better to be ignored. The human factor is often seen as an enemy of information security, statistics showing that in many cases employees act maliciously or through

negligence on data integrity without paying attention to internal security procedures. The education of staff regarding information protection requires time, effort and budget and the results are not encouraging meaning that often the staff is not interested in this direction.

Research and studies undertaken so far, the solutions offered by providers of BI tools come with different approaches on improving information security by:

- Establishing clear criteria in selecting suppliers of cloud storage facilities
- Protecting data before storing in the cloud
- Information access control
- Information Control
- Creating a culture of information security within organization

Establishment of clear criteria in selecting suppliers of cloud storage facilities

Depending on user requirements, there are three broad categories of storage services on the market:

IaaS (Infrastructure as a Service) - provider handling a rented and complex technology infrastructure which can span multiple geographic areas. The level of security offered doesn't go beyond protecting the infrastructure itself and the operating systems, applications and content will be managed and secured by the user.

SaaS (Software as a Service) - supplier offering various applications to end users via web: spreadsheets, word processing records, register of shared mail, etc. The security offered is relatively high, the supplier having an important responsibility task on the line of security.

PaaS (Platform as a Service) - provider offering advanced solutions and applications hosting. Thus there is little need for user to have specific additional hardware or software internally. Through this offered flexibility, there is the possibility of integrating an additional layer of security.

Cloud storage feature presents obvious benefits, but carries security risks also. Two of the biggest fears in adopting cloud methods are unauthorized access to information held and security flaws. Security and privacy issues are generated because of the fact that data is located in different jurisdictions with different levels of protection. Guidelines developed by the National Association for Information Systems Security – "Security in the cloud" advance the idea of ensuring

information in the cloud computing environment through three levels of security [7]:network security, server security, and application security

In each case there are solutions which can be adopted in advance in order to prevent such shortcomings.

Cloud storage providers must ensure that they have a safe infrastructure, client's data and applications are protected and supply disruptions in the system are minimized. In turn, client companies must avoid vendors who refuse to give details about their security programs. A study by Gartner highlights some issues to be considered in selecting a cloud provider:

- Privileged access to data: Who handles customer data?
- Respect for the rules: Are external audits conducted or safety certifications valid?
- Location of data: Where to store data?
- Data segregation: It provides encryption? What exactly is in the process of segregation of data?
- Recovery: What happens in case of disaster?
- Investigative Support: are there any illegal activities?
- Validity term: it is possible to recover data in case of necessity?

With the gathered information regarding the selected cloud operator, the client organization shall ensure that, at least, the conditions offered by traditional data storage are fulfilled.

Protecting data before storing in the cloud

Given previous recommendations, companies using cloud services have a range of measures that can minimize security risks. Once storage provider is selected, relatively simple steps can browse in order to identify the information user:

• Knowledge: something only the user knows (password or PIN);

• Possession: something only the user has (magnetic card or token); and

• Inherence: something only the user is (fingerprint or voice).

The variant of encoding or encrypting messages or information can be taken into consideration and this is how data can be read and processed only by authorized user. Of course, companies providing cloud services can offer encryption but there is also the possibility of undesirable decryption. By encrypting

data before transfer to the cloud ensures that access is unlikely without the decryption key [10].

Information access control

It is well known that everybody wants to access the needed information in a fast manner and from various devices and from various places. Of course, BI tools claim to be a clever solution for this task but also, these instruments carry a lot of vulnerabilities. Accelerated development of the mobile terminals (phones, laptops, tablets) brings a number of security vulnerabilities of BI tools. Users tend to have mobile access to everything in the office for reasons of efficiency including the use of BI capabilities in this way. Mobility puts sensitive data for an organization to be combined with personal data, so a mixture of information occurs on the same terminal [9].

Securing Business Intelligence facilities primarily involves a rudimentary technique: the application of controlling the access to information. So:

- Users can get permission to access only the data required or that are dedicated to them. Obviously analysis or processing of data or information not concerning a user by error may have totally irrelevant results and could also be serious security vulnerability.

- Access can be granted directly to the data warehouse or only to reports or presentations. This dilemma occurs quite frequently within entities and is a subject of intense debate among analysts involved in the field. It is clear that in terms of information security and, sometimes, quite complicated bureaucratic procedures it is safe to limit access only to reports and presentations. It appears, however, the disadvantage that many users of BI tools access the same information or data - in fact counter-productive - and management waste precious time on security details and procedures.

Another major data security risk is the loss or theft of the mobile terminal. In such situations, legal notices on occurred security breaches are recommended. The variant in which the mobile device has offline capabilities implies data theft risk and, therefore, Business Intelligence applications should avoid local copies of data retention. In this case, encryption is a welcomed security measure.

The implementation of a security policy in the area of BI can be based on several factors:

- Data classification - establishing data "sensitive" in terms of BI capabilities and, therefore, measures should be taken to protect them. There may be several levels of sensitivity that may require specific measures.
- Classification BI users facilities - is performed depending on the position and role within the organization.
- Standardization of rights - determines how BI tools are allowed to access data and perform specific functions.
- Transmission – it refers to encryption and the authorization levels are established for access and file transfer.
- Data storage - permitted storage locations and manner of back-up are taken into account.

Information control

The goal of all processes related to information control (exercised by human or system) is getting its veracity by achieving predetermined quality standards [3]. These approach methodologies are grouped into three categories:

- intra-system control - exercised within a system or application. It is characterized by an existing logic and follows the organization's needs.
- inter-system control - check data integrity between systems validating actually an exchange of information.
- transactional balance control - include both of the above. It captures data errors that occur in the systems but also during data transfers. Such control is quite difficult to achieve due to the initial set up that requires extra time and effort.

In all variants presented it is essential that these procedures are non-intrusive (to act independently of monitored systems) and have a flexible logic (to have the ability to verify, balance, reconcile and track data).

Implementing an appropriate control of information must be supported by a series of internal factors of which the most relevant are: support from executive level, internal partnership and existence of a plan of action.

As the main beneficiary of BI tools, the executive level makes budgets, supports, implements and maintains control policies. Decision makers have a top-down approach on work processes and can impose control information.

Internal partnership aims at a common approach by the departments involved in control policies (IT, audit, ownership, etc.) even if there are different

views on the desired outcomes, costs or methodologies. It is essential to have a collection and proper symbiosis of all existing views in this respect in an organization in order to avoid internal policies and regulations reversals or delays in ongoing projects.

The existence of a proper plan is based on a correct drafting of current processes within an entity, with all their characteristics (information flows, current controls, incomplete analyzes, lack of conclusive data or excess/ballast of information).

Information security culture

The culture within an organization can be defined as the way activity goes at various levels within an entity. This term encompasses beliefs and values essential to the conduct of the members and may confer a competitive advantage through business excellence, product quality, customer satisfaction, partners' engagement and employee mobilization. This last aspect plays a decisive role and translates into behaviour within the organization which helps protect data, information and knowledge, and which includes perceptions, attitudes, assumptions and beliefs about information security.

Creating and implementing a proper information security within an organization primarily involves creating a culture in which all users, at all levels and departments, understand threats and security procedures, acquire active practice in this regard, take decisions based on the protection of information and understand the information security as an integral part of their service prerogatives [5].

National Association for Information Systems Security (ANSSI) of Romania defines in the *Code of Proper Practices for Information and Communication Systems Security* [6] a set of recommendations for an entity management and other employees. Thus, information system security is seen as a responsibility belonging to the management structures, who are expected to provide a clear direction in this regard by undertaking the following actions:

a) Review and approve the security policy and establish related responsibilities;
b) Monitore significant changes in exposure of information system to major threats;
c) Review and monitor information system security incidents;
d) Approve measures to improve information security.

Policy makers are given a list of directions to follow in order to emphasize the human resource, beginning with the recruitment stage, up to training programs for IT specialists and beyond. Furthermore, regarding the management levels in charge of the information protection, two strands are becoming increasingly important: *implementing an information security culture* and *BI facilities*. The latter ones primarily intended for collection, storage, knowledge management through analytical methods providing solid information for decision. Role of BI tools to improve data transparency and visibility eventually translates into information security monitoring and sustain development of an information security culture within an organization.

Implementation of such an organizational culture entails two specific dimensions of the human factor: *knowledge* and *behaviour*. The in-company training programs must aim not only at training, but also human resource modeling in order to comply with internal policies, with emphasis on data protection procedures. The aim is to induce an employee appropriate behaviour in order to respect and ensure the information security through the pursuit of knowledge and the application of proper practices.

IT departments play the key role in providing management speedy information in the required form. The quality of the specialist's work is influenced by the volume of processed data and by available resources in the company. This is why a higher level of information security is also a result of the infrastructure meaning platforms, applications, servers, procedures, etc.

Case study

In 2009, the Rompetrol company decided to change strategy through consolidation of the management process and of the IT system optimization. Internal analysis revealed thatthere was a low level of CPU usage, there was no virtualized environment for optimizing servers loading and there was no solution available for disaster recovery for the whole system. By choosing the SAP application, the organization decided to replace the IT Business Units, which had too many slow-working and asynchronous servers, platforms and applications, with a Vblock solution, provided by an alliance between Cisco, EMC and VMware.

The result was a unique platform combining the best solutions regarding information handling , namely information processing, storing, administration and

security. The integration of servers, operating systems and business applications (Business Intelligence, ERP, CRM) led to financial (Return on Investments of 22 %, Internal Rate of Return of 64 %) and operational advantages (reduced operational costs, higher level of hardware availability and CPU usage). In the new conditions, human resource gained efficiency due to improved speed of response from IT department and also to 50 % reduction of workload of IT team.

These results, related to a complex virtualization process made in a private cloud that hosted a successful IT & C solution, proved to be essential for management in terms of efficiency and security [8].

The management is responsible to recruit proper human resources and also to create conditions for modelling employees in the spirit of organizational needs in the field of security. Obviously, knowledge is fundamental but it should be used and directed to the common interest that should be a safe information flow. This is why behaviour is essential and must be determined by the awareness of the fact that individual benefits are determined by the company's results. Business Intelligence tools measure performances at various levels: on different products or services, on individuals or teams and may provide a strong starting point for establishing strategies or future policies. In fact, these are internal analysis based on information issued by different departments or organizational levels and from different terminals. The whole process is marked by the human touch, which is essential because the system (hardware, software, applications, etc.) must be "fed" and maintained with safe and quality data.

4. CONCLUSION

Business Intelligence tools have evolved and tend to keep up with current challenges existing in public and private sectors. The market offers designed by providers regarding such instruments is more varied and adapted, supporting decision makers through integrated solutions and processing capabilities, reporting, presentation and storage, all being attractive in terms of costs and flexibility.

Thus, the BI user should have a positive general picture: quick access to the needed information from anywhere, friendly and suggestive charts or dynamic reports, analysis of trends, KPI's evolution, sales and margin analysis, budget status ,

etc., all at a click distance. However, these facilities may hide threats that are often forgotten or not seriously taken into consideration by literature or BI providers.

It remains a real challenge to ensure protection of information at all stages of BI-specific flow. Now regarded as a basic resource for an enterprise, information held should be clean, consistent and able to provide confidence to managerial act. In this regard, the solutions promoted by software providers and literature converge on the idea of implementing strict and clear policies and procedures. When a company decides to step into the path of BI tools and cloud solutions, the issue of information security becomes a priority and, at the end of the day, it turns into Business Intelligence security. So far, research focused mainly on technical solutions, all requiring more costs and, in many cases, leading to few results. This is why Business Intelligence instruments may fail in their initial task by becoming untrustworthy applications.

Thus, the big question is: What does it take for a company to implement a secure BI solution? Does it require additional costs to ensure a safe information flow, or more attention should be paid to the human factor?

Beyond written rules, this paper suggests a greater focus on human resources during the BI tool implementing steps: from the evaluation of the initial information flow to the final desired reports and analyses. Involving all human resources is a smart thing to do due because the employees are supposed to gather data, introduce it in the system, follow procedures, maintain a certain discipline and permanently evaluate the results. It should be more sustainable and profitable on long term to induct a proper organizational culture in order to keep the fundamental values of the company always alive.

A culture of information security that is actively supported by management can help users understand the concept of data protection and BI tools in use.

The range of BI applications must adopt functions in order to ensure information integrity. The developers of such systems are already in the position to create flexible architectures adapted to this end and to establish confidence in the final product.

BIBLIOGRAPHY

1. D. Airinei, "Depozite de date", Editura Polirom, Iasi, 2002.
2. D. Airinei and D. A. Berta, "Semantic Business Intelligence – a New Generation of Business Intelligence", Informatica Economica [Online]. 16(2/2012). Available at http://revistaie.ase.ro/content/62/08%20-%20Airinei.pdf

A. DeBroux and C. Reed, "How to Build Trust in Your Data Warehouse", Business Intelligence Journal [Online]. 20(1/2015) Available at https://tdwi.org/~/media/FC16C9880A4141868CA20AE5F383EB92.pdf

3. V. T. Nandi, "Maintaining Database: Business Intelligence Tool for Competitive Advantage", Business Intelligence Journal [Online]. 5(2/2012). Available at www.saycoroprativo.com/saycoUK/BIJ/journal/Vol5No2/Article_17.pdf

4. C. Paulsen and T. Coulson, "Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security", Communications of the IIMA [Online].11(3/2011). Available at scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1169&context=ciima.

5. https://www.cert-ro.eu/files/doc/729_20130401030415043075400_X.pdf
6. https://www.cert-ro.eu/files/doc/775_20131030091057011764400_X.pdf
7. http://www.crescendo.ro/iqon-si-crescendo-implementeaza-platforma-%E2%80%9Cvblock%E2%80%9D-intr-un-proiect-de-consolidare-a-it-ului-in-cloud-premiera-in-europa-de-sud-est/
8. https://www.grtcorp.com/solutions/data_warehouse_business_intelligence/bi-security
9. http://mobile.datamation.com/cloud-computing/can-you-secure-your-business-intelligence-data-in-the-cloud.html