Metadata of the chapter that will be visualized in SpringerLink

Book Title	Developments and Advances in Defense and Security
Series Title	
Chapter Title	Empirical Study of the Application of Business Intelligence (BI) in Cybersecurity Within Ecuador: A Trend Away from Reality
Copyright Year	2018
Copyright HolderName	Springer International Publishing AG, part of Springer Nature

Author	Family Name	**Andrea Vaca**
	Particle	
	Given Name	**H.**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador
	Email	andrefa6@hotmail.com
Corresponding Author	Family Name	**Reyes Ch.**
	Particle	
	Given Name	**Rolando P.**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador
	Division	Departamento de Seguridad y Defensa
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador
	Email	rpreyes1@espe.edu.ec
Author	Family Name	**Vaca**
	Particle	
	Given Name	**Hugo Pérez**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador
	Division	Departamento de Seguridad y Defensa
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador

	Email	hlperez@espe.edu.ec
Author	Family Name	**Paredes**
	Particle	
	Given Name	**Manolo**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador
	Email	dmparedes@espe.edu.ec

Abstract	Business Intelligence (BI) over the years, has achieved a strong impact within the business world, especially when it comes to gaining knowledge for making strategic decisions. This impact has been successfully in other contexts. However, only exist some examples in Latinamerica (Costa Rica), have started to use BI for the Cybersecurity context, being a strange when several authors have considered this relationship as a global trend. Our objective is to investigate if this trend is happening in Ecuador. For which, we propose to carry out a survey to professionals in the industry and professors in the academy. The results obtained show that the majority of Ecuadorian companies, use BI only to improve their competitiveness, but without considering cybersecurity context, despite being aware of the high risk. The industry, academia and country must enter a stage of reflection of the application of BI in Cybersecurity.

Keywords (separated by '-')	Business intelligence - BI - Cybersecurity - Survey - Trend

Empirical Study of the Application of Business Intelligence (BI) in Cybersecurity Within Ecuador: A Trend Away from Reality

H. Andrea Vaca[1], Rolando P. Reyes Ch.[1,2](✉), Hugo Pérez Vaca[1,2], and Manolo Paredes[1]

[1] Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
andrefa6@hotmail.com,
{rpreyesl,hlperez,dmparedes}@espe.edu.ec
[2] Departamento de Seguridad y Defensa, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador

Abstract. Business Intelligence (BI) over the years, has achieved a strong impact within the business world, especially when it comes to gaining knowledge for making strategic decisions. This impact has been successfully in other contexts. However, only exist some examples in Latinamerica (Costa Rica), have started to use BI for the Cybersecurity context, being a strange when several authors have considered this relationship as a global trend. Our objective is to investigate if this trend is happening in Ecuador. For which, we propose to carry out a survey to professionals in the industry and professors in the academy. The results obtained show that the majority of Ecuadorian companies, use BI only to improve their competitiveness, but without considering cybersecurity context, despite being aware of the high risk. The industry, academia and country must enter a stage of reflection of the application of BI in Cybersecurity.

Keywords: Business intelligence · BI · Cybersecurity · Survey Trend

1 Introduction

Business Intelligence (BI) is an approach that is not new, within the global trend. Since its inception, it has been used to transform the company's data into important information to get later into knowledge [1]. However, in recent years, this focusing has managed to maintain an interesting trend where currently BI tools allow performing systematic and controlled processes for generation of knowledge in aggressive business strategies to the companies [2]. That is why; it is not uncommon to find BI in other fields of application such as: knowledge management, analytics, and cybersecurity, among others. For the particular case of BI in cybersecurity, it is still new, at least in Latin America, except for a specific case in Costa Rica [3]. In Ecuador, BI focus on cybersecurity is practically unknown, although it seems that BI's application is oriented only business part. For this reason, our objective in this empirical study is to establish the current state of the applied BI approach in cybersecurity in Ecuador, and to establish if its application is appropriate within companies and academia. We apply a

Á. Rocha and T. Guarda (Eds.): MICRADS 2018, SIST 94, pp. 1–9, 2018.
https://doi.org/10.1007/978-3-319-78605-6_1

methodology of quantitative research based on a survey, which we were done to professionals and academics. The results indicate that BI is not applied in cybersecurity and that only is being used for reports and analytics in business transactions. In Ecuador, a period of reflection is needed to improve the application of BI in cybersecurity in order to increase prevention.

The present article consists of the following: Sect. 2 describes the background that refers to the research topic. The methodology used and research questions are detailed in Sect. 3. In Sect. 4, execution and results are mentioned. The discussion and conclusions are set out in Sect. 5. Finally, Sect. 6 indicates future work.

2 Background

According to Journal & Conscience [4], Business Intelligence (BI) was used to obtain and collect business transactional information in order to create knowledge or predictions that allow executives or directors to make decisions. Obtaining this type of information required considerable time and specialized personnel. However, at present, Business Intelligence (BI) has advanced a lot in this aspect, to such an extent that now it has software tools that have allowed companies to reduce the time of processing their information to make decisions instantly. The companies have been able to generate more quickly, useful and necessary knowledge of their business, creating competitive advantages in the short and long term [5]. To explain about what BI represents, we will make a brief description of the current situation of BI in the world and its incursion in cybersecurity.

AQ3

2.1 Business Intelligence Systems and Their Field of Application

According to Barrento et al. [2], a Business Intelligence (BI) system is an integral solution that includes several software tools; allow collecting the largest amount of information, any type of data such as: empty or duplicate data, in order to transform them into information readable that the user can analyze and observe through graphics, among others. The author tells us that the trend of the field of application of BI is strongly linked to:

- **Knowledge Management:** with which has allowed creating useful knowledge for the administration, learning and regulatory compliance of a company.
- **Collaboration platform:** which has allowed the facilities to obtain information from various areas and exchange them with each other based on their data.
- **Reports or reports:** This has improved the visualization of information at a dynamic level or understandable to a normal user, in particular the users who represent the top managers of an organization or Company.
- **Analytics:** to establish quantitative processes in the aid of optimal decision making. At this point is where we consider the terms of: process mining, the generation of patterns from large volumes of data [6], process mining, process management techniques through events [7] and the well-known statistical analysis, which allows investigating individual or collective data samples.

- **Measurement:** This has allowed the creation of hierarchies in performance measures. The measures are commonly used by employers as indicators to determine the status of a company.

2.2 Management of Large Volumes of Data in Cybersecurity

Cybersecurity according to ISACA [8] it is defined as a set of instruments, strategies, knowledge, norms, risk techniques, alignments, experiences and technologies that are strongly related to safeguarding the assets of the organization and users with respect to external intrusions.

In this regard, we can say that thanks to this concept by ISACA, it is reasonable to see that there is currently a large deployment of tools, policies for cybersecurity. Its reason seems to be obvious, because it is a discipline that operationally generates large volumes of information, which could even be said that there are cases where obtaining information is such, that it may have exceeded the capacity of the usual software (e.g., malware-attack). This is the main reason, for management of large volumes in cybersecurity is necessary and paramount when processing information in a reasonable time [9].

In a study conducted by Mondrag [3], tells us that the information of the companies about of cybersecurity refers mostly to cyber-attacks; among the most common we can say: denial of service, port scanning, and malware propagation, among others. What the companies have done in this regard, is to use BI tools as a strategy for the visualization of interpretive graphs of the attacks (histograms, cakes, bars) in real time. The author considers that in this aspect, BI tools are useful to generate patterns that they can be visualized instantly as a means of preventing new cyber-attacks or compare with other attacks or establish regulations and organizations' rules that endorse the proper protection.

2.3 Cybersecurity and Visual Representation of Patterns Based on Large Volumes of Data

According to Arias [10], the construction of patterns from information of the computer attacks provided by a BI tool, have helped companies and academies to create knowledge to prevent and take care of their assets, as well as to create procedures for the protection of its information. A case of this conclusion, the author refers to BI's tendency using in cybersecurity within several Costa Rica companies. The reason is simple, BI techniques have allowed them to transform the information obtained from a cyber-attack, or from a simple data set, to knowledge and prediction of future cyber-attacks [11].

2.4 Cybersecurity and Its Trend in Ecuador

According to Ekos Journal [12], Ecuador companies, in recent years, have begun to evolve their business models thanks BI use, obtaining competitive advantages, improving their added value and creating new business scenarios in real time, fully predictive, based on appropriate decisions to grow their business. This magazine predicts the possibility that companies, over the years, improve BI's concepts within their businesses to match the global trend. However, while commercial experts find themselves boasting about BI use in their businesses, Vargas et al. [13], warn that in recent years, Ecuadorian companies have had cyber-attacks on their assets, being especially alarming in the banking sector due to the few and limited measures that the Ecuadorian government is taking in this regard.

According to what has been found in the literature, we can deduce that BI is a trend which is growing up in the world, especially in business issues, when obtaining competitive strategies. In Ecuador, BI trend has not been the exception. However, the world has started to use the BI approach in several aspects of cybersecurity, a situation that is possibly a distant and unknown issue in Ecuador. So, we ask ourselves, if the BI approach applied in cybersecurity in Ecuador, is the right one within the companies and the academy, considering the current trend. For which, we have raised the following research questions:

RQ1: Is the BI approach and its tools being used as part of the research techniques for cybersecurity within companies and academia in Ecuador?
RQ2: Which is the recent status of BI application, and how are they being associated in cybersecurity in Ecuador?

3 Research Methodology

The research questions previously mentioned raise a survey as a research strategy (quantitative). The survey elaboration and application, we consider the recommendations of Monterrey [14], who establishes 7 stages for the application of the survey, in which we used all the stages of Monterrey [14], because it fits our research. To detail in the Fig. 1, it shows the stages of the research methodology. AQ4

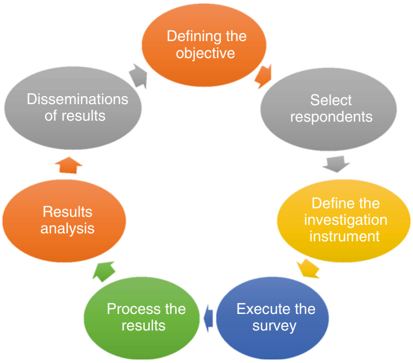

Fig. 1. Research methodology

In this regard, the stage of *defining the objective* is oriented to what the researcher wishes to investigate in his research questions. The research questions were defined in Sect. 2. The next stage refers to *selecting the respondents*, where we select our respondents from different companies and academies in Ecuador at random way. The selection of company respondents is aimed at people working in systems departments of public and private companies in Quito city, and with respect to respondents from the academy, it was appropriate to select teachers who know issues related to cybersecurity or BI. For the stage called *determining the instrument* refers to practically survey preparation with 7 questions, where 1, 2 and 3 respond to our RQ1 and questions 4, 5, 6 and 7 respond to our RQ2. The *survey execution* is the application of the survey to the selected respondents. The *processing and analysis of the results* is done with Google tools, and finally the dissemination of the results that is done in this article. The results of the execution of the methodology are detailed in the following section.

4 Execution and Results

4.1 Execution

As mentioned above, the selection of respondents was oriented to public companies that have considerably large computer infrastructure, a situation that also we take into account regarding the academy. The survey was sent by email to a total of 50 respondents, of which 30 are distributed to professionals who belong to private companies, 16 to professionals from public companies and 4 surveys sent to professors of the Academy. The survey was applied during 2 months at the end of the winter of 2016. In total, 47 respondents answered, representing a 94% response rate, considered acceptable in this type of studies.

4.2 Results

RQ1: Is the BI approach and its tools being used as part of the research techniques for cybersecurity within companies and academia in Ecuador?

To answer this research question, it is necessary to initially inquire with information regarding the “use of research techniques and BI tools in the company/academy”, where it can be observed (Fig. 2) that 56.5% of respondents affirmatively use research tools and business intelligence solutions, 39.1% of respondents barely know some references and 8.7% have total ignorance of the subject. In addition to the results of this question, we also consider asking the respondents (who answered affirmatively to know BI) if the tools they use are free, proprietary or self-developed (Fig. 3). Results indicate that 50% of respondents use free software tools, 39.1% prefer proprietary software and few respondents develop their own tools (6.5%).

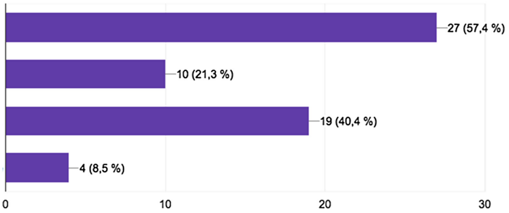

Fig. 2. Use of research techniques and BI tools in companies/academy

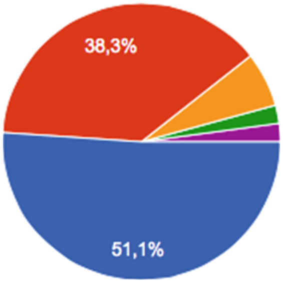

Fig. 3. If you use BI tools, what characteristics are they?

We inquired by asking respondents if they had any difficulty acquiring BI tools. Figure 4 shows that 58.7% consider difficulty in acquiring BI tools due is in its high cost, 43.5% consider not knowing the advantages of the tools to acquire those, 34.8% think that the lack of training can influence, and 15.2% consider the difficulty of finding support.

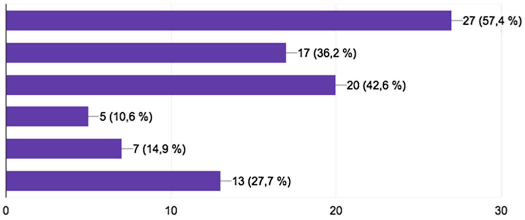

Fig. 4. What do you think would be the main difficulty in using BI tools in your business?

RQ2: What is the status of BI application, and how are they being associated in cybersecurity in Ecuador?

To answer this research question, we considered asking the respondents if they use their Business Intelligence (BI) tools for any particular reason (e.g., fraud, statistics, etc.). Figure 5 shows that 39.1% of respondents mention that they use BI tools to find business characteristics that improve their competitive strategy, 32.6% of respondents

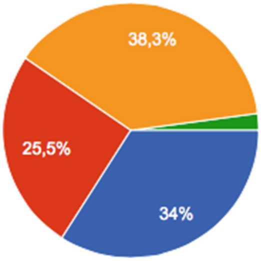

Fig. 5. You think that BI tools or solutions are a great help for?

used for the detection and prevention of computer frauds, 26.1% very closely appears of respondents that used in statistical and economic analysis and only 2.2% for other purposes.

We are very interested in who responded about using BI tools to detect fraud. We wanted to ask, if the company or academy create internal policies for the use of BI tools. Figure 6 shows that 52.2% of companies/academia have not elaborated policies for the use of BI tools, 32.6% have elaborated policies but only related aspects of the business turnaround and only 26.1% have tried to perform internal policies but related to cybersecurity.

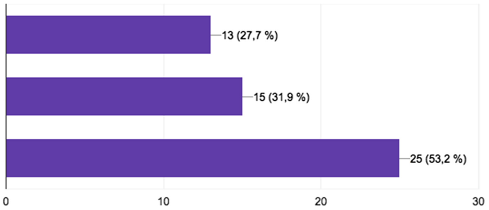

Fig. 6. Where do you work, have you developed internal policies for the use of BI or cybersecurity tools?

With this information we can complement our inquiry, when we ask the respondents, if there is an effective application of their policies. Figure 7 shows that 63% believe that effective training and dissemination is necessary for use, 52.2% think that effective application believes that a national cybersecurity policy is necessary, while

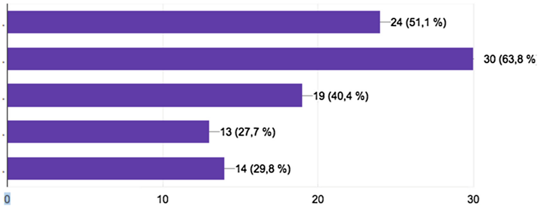

Fig. 7. What do you think is necessary for a proper application of BI tools policies in cybersecurity?

41.3% think that effective application is necessary a national program of diffusion in the use of the tools or solutions of BI within the context of cybersecurity.

Finally, we asked the respondents if authorities, to which they belong, are aware of information security risks and if they know how to mitigate them (Fig. 8). The 34.8% are very aware of the risks of computer attacks on companies, 26.1% mention that they are aware, but do not know how to mitigate the risks, 21.7% are also aware, but are not interested in their safety of information, and finally 17.4% are not aware nor are they interested.

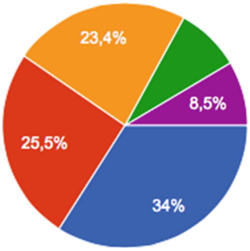

Fig. 8. The institution to which they belong, are aware of the risks in information security and how to mitigate them?

5 Discussion and Conclusions

The results obtained are really interesting as well as worrisome. Ecuadorian companies are using BI tools with the main objective of giving greater added value to their business with the perspective of improving their income. The discussion is clear, in Ecuador, research techniques and BI tools are only oriented to improve the economic companies' environment. Although, these tools, for Ecuadorian companies are extremely useful for their decision making, companies do not invest in them, but opt for the use of free software tools, where they do not pay maintenance subscriptions and updates. Regarding the perspective of using their BI tools in the context of cybersecurity, companies are not interested in investing in this aspect, despite of the fact knowing the risks and opening up possibilities of becoming potential targets of cyber-attacks. We believed, if companies did not use their BI tools in their cybersecurity they could at least have policies in that regard. But to our surprise, internal policies have not been created for the use of BI tools and even worse for cybersecurity, even though managers are aware of the risks. We believe that initiatives should be taken regarding the use of BI tools in cybersecurity since they allow in some way to prevent computer attacks. It is strange to know that the companies are waiting to earn more money while are exposed to being attacked and losing their biggest investment. For this reason, companies must take the initiative to take care of their investments establish internal policies, until the Ecuador's Government defines and presents national cybersecurity policies, Ecuador's companies and academia must enter a period of reflection in this regard.

6 Future Works

Our research leads us to several future works, among which we can mention the creation of a proposal for internal business policies in the BI environment in cybersecurity context. Additionally, the creation of national cybersecurity policies with the use of BI tools possibly created as a proposal by the Ecuadorian State. To this, we can add research concerning the creation of algorithms that obtain patterns of computer attacks using BI tools, among others.

References

1. Perspectiva, R.: Las nuevas tendencias de la inteligencia de negocios. [online] IDE Perspectiva (2018)
2. Barrento, M., Neto, M., Maria, M., Dias, S.: Sistemas de Business Intelligence Aplicados à Saúde (2010)
3. Mondrag, G., Guzm, C.A., Mart, L.: Revisión Sistemática de Literatura: Visualización de Seguridad (n.d.)
4. Calzada, L., Abreu, J.L.: El impacto de las herramientas de inteligencia de negocios en la toma de decisiones de los ejecutivos. Int. J. Good Consience **4**(2), 16–52 (2009)
5. Cano, J.L.: Business Intelligence: Competir Con Información, p. 397. Banesto, Fundación Cultural (2007)
6. Riquelme, J.C., Ruiz, R., Gilbert, K.: Minería de datos: Conceptos y tendencias. Inteligencia Artificial **10**(29), 11–18 (2006)
7. Pérez Jiménez, S.: Minería de procesos (2015)
8. ISACA: Cybersecurity Fundamentals Glossary (2014)
9. Jiménez, L., Hernandez, S., Mendez, J.: Enfoque Sociotécnico Aplicado a un Sistema de Gestión Business Intelligence (n.d.)
10. Arias, R., Leiva, C.: Representación visual de patrones de ataque en ciberseguridad (n.d.)
11. Laudon, S.: Sistemas Informacion (1999)
12. Ekos Revista, La inteligencia en el negocio (2016). http://www.ekosnegocios.com/negocios/. Accessed 18 Jan 2018
13. Vargas, R., Recalde, L., Reyes, R.: Ciberseguridad. Ciberdefensa Y Ciberseguridad, Más Allá Del Mundo Virtual: Modelo Ecuatoriano de Gobernanza En Ciberdefensa **20** (2017)
14. Universida Virtual del Tecnológico de Monterrey: Metodología para llevar a cabo una encuesta (2005)

Author Query Form

Book ID : **462684_1_En**
Chapter No : **1**

Springer
the language of science

Please ensure you fill out your response to the queries raised below and return this form along with your corrections.

Dear Author,
During the process of typesetting your chapter, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided below

Query Refs.	Details Required	Author's Response
AQ1	Please confirm if the corresponding author is correctly identified. Amend if necessary.	
AQ2	Please check and confirm the edit made in "Affiliation 2".	
AQ3	Please confirm if the section headings identified are correct.	
AQ4	Kindly note that, to maintain sequential order figure numbers are renumbered both in figure captions and in the text. Kindly check and confirm.	

MARKED PROOF

Please correct and return this set

Please use the proof correction marks shown below for all alterations and corrections. If you wish to return your proof by fax you should ensure that all amendments are written clearly in dark ink and are made well within the page margins.

Instruction to printer	*Textual mark*	*Marginal mark*
Leave unchanged	• • • under matter to remain	ⓥ
Insert in text the matter indicated in the margin	⋀	New matter followed by ⋀ or ⋀ⓧ2
Delete	/ through single character, rule or underline or ⊢——⊣ through all characters to be deleted	₰ or ₰ⓧ2
Substitute character or substitute part of one or more word(s)	/ through letter or ⊢——⊣ through characters	new character / or new characters /
Change to italics	— under matter to be changed	⌙
Change to capitals	≡ under matter to be changed	≡
Change to small capitals	= under matter to be changed	=
Change to bold type	∼ under matter to be changed	∼
Change to bold italic	≂ under matter to be changed	≂
Change to lower case	Encircle matter to be changed	≢
Change italic to upright type	(As above)	⊹
Change bold to non-bold type	(As above)	⊹∼
Insert ‘superior’ character	/ through character or ⋀ where required	Y or ⋏ under character e.g. $\overset{2}{Y}$ or $\overset{2}{\curlywedge}$
Insert ‘inferior’ character	(As above)	⋀ over character e.g. $\underset{2}{\wedge}$
Insert full stop	(As above)	⊙
Insert comma	(As above)	,
Insert single quotation marks	(As above)	$\overset{‘}{Y}$ or $\overset{‘}{\curlywedge}$ and/or $\overset{’}{Y}$ or $\overset{’}{\curlywedge}$
Insert double quotation marks	(As above)	$\overset{“}{Y}$ or $\overset{“}{\curlywedge}$ and/or $\overset{”}{Y}$ or $\overset{”}{\curlywedge}$
Insert hyphen	(As above)	⊢-⊣
Start new paragraph	_⌐	_⌐
No new paragraph	↩	↩
Transpose	⊔⊓	⊔⊓
Close up	linking ⁐ characters	⁐
Insert or substitute space between characters or words	/ through character or ⋀ where required	Y
Reduce space between characters or words	| between characters or words affected	⊤