Cyber risk: An analysis of self-protection and the prediction of claims

Alana K. Azevedo [1,2], Alfredo D. Egídio dos Reis [1] & Agnieszka I. Bergel [1]

[1] CEMAPRE & ISEG - UNIVERSIDADE DE LISBOA
[2] UNIVERSIDADE FEDERAL DO CEARÁ

2021 - ASTIN Online Colloquium
18-21 may 2021

Summary

Introduction

The evolution of business relationships through digital platforms raises concerns about cyber security.

Several ways to mitigate this risk were already widespread in this virtual environment, such as antivirus, firewall, data protection, authentication technology, secure communication, access restriction.

Many countries are already concerned with defining policies that involve cybersecurity standards, including Brazil, a country with substantial geographic and population dimension, consequently, exposed to great vulnerability.

Cyber risk scenario in Brazil

- In 2014 Brazil was ranked as number one in the world for banking malware attacks, with nearly 300,000 compromised users, Muggah & Thompson (2017);
- At least 75 per cent of Brazilian Internet users claim to have been victims of some form of cyber crime, Diniz *et al.* (2014);
- Ponemon Institute (2019) allocates Brazil in the first position of the ranking of probability of data leakage. This probability of data leakage is 43%.

Motivation

Motivation

- Despite the existence of several forms of security measures against cyber attacks, the risk of both financial and operational losses is still considerable.
- This paper proposes an analysis focusing on the occurence of claims, in the light of individual characteristics of Brazilian companies in relation to the use of technologies and cyber risk management.
- Does security protection help to prevent cyber attacks?
- Is it possible to predict the occurrence of claims and to generate information about companies that may have high cyber risks attacks?

Objective

Our objective is to shed new light on cyber risk, by measuring the difference on the number of claims of similar companies with and without security protection against cyber risk. To achieve this goal, we undertake a sample of companies and apply a propensity score-matching method which involves pairing treatment and comparison units that are similar in terms of their observable characteristics.

Using these same characteristics, we develop a neural network system to predict the occurrence of claims and offer an innovative way as a support tool for better identification of the specific condition of the company about cyber risk.

Literature Review and Background

The key to an efficient mitigation of cyber risks is the assessment of all basic knowledge about the Information Technology (briefly, IT), the structuring of digital assets, the interconnected environment and the level of existing outsourcing.

Ogut *et al.* (2005) analyzed firm's IT security risk management strategies when their risks are interdependent. Only the interdependency that arises due to of interconnections of computers in different firms was modeled.

Literature Review and Background

One important approach used in some cases of cyber risk analysis is the copula model. Copulas are functions that join or couple multivariate distribution functions to their one-dimensional marginal distribution functions. It has great value for modeling dependent risks.

Mukhopadhyay *et al.* (2006) developed a framework, based on copula aided Bayesian Belief Network model, a graphical relationship between causal variables, to quantify the risk associated with online business transactions, arising out of a security breach.

Propensity score matching

The purpose of using propensity scores and a matching algorithm in this work is to produce an unbiased causal effect using observational data regarding the acquisition of cyber risk security protection and its impact on the number of claims.

Definition [Rosenbaum & Rubin (1983)]

Conditional probability of assignment to a particular treatment given some vector of observed covariates. Let X denote the vector of those covariates for a particular company, and let the binary variable T indicate whether the company was exposed ($T = 1$) or unexposed ($T = 0$). The propensity score, $e(x)$, is the conditional probability of exposure given the vector x of covariates.

Neural network

Definition

To briefly define a neural network we considered the definition of Gallant (1993) that stated that a NN model consists of a set of computational units and a set of one-way data connections.

According to Svozil *et al.* (1997), the main advantage of neural networks is the fact, that they are able to use some a *priori* unknown information hidden in data (but they are not able to extract it). The power to observe each aspect of the data set and how its units may or may not relate, gives neural network the ability to determine complex patterns across diverse volumes of data.

The Data

The Brazilian Institute of Geography and Statistics (IBGE) is the main provider of data and information in the country.

In the year 2010, the research on the use of Information and Communication Technologies (ICT) investigated aspects of the use of these technologies by the Brazilian business segment. We considered only the information of companies that used computers and the internet, a total of 16,725.

The first variable used in data design was the number of security measures adopted by companies against cyber risks.The second variable, the outcome variable, was the number of Claims.

In addition, our research presents another 16 statistically significant variables related to companies that used the internet in the period considered.

Definition of covariates

Variables	Definition
Depart	Set to 1 if the company owns IT department, 0 otherwise
Quali	1 if the company provides IT qualification, 0 otherwise
Security	1 if the company has IT security policy, 0 otherwise
Wired	1 if the company has wired local network, 0 otherwise
Wireless	1 if the company has wireless local network, 0 otherwise
Intranet	1 if the company has intranet, 0 otherwise
Extranet	1 if the company has extranet, 0 otherwise
Cloud	1 if the company has used cloud computing, 0 otherwise
Readysoft	1 if the company uses out-of-the-box software, 0 otherwise
Freesoft	1 if the company uses free software, 0 otherwise
Othersoft	1 if the company uses software developed by another company, 0 otherwise
Homepage	1 if the company owns homepage, 0 otherwise
Fixed	1 if the company uses fixed broadband internet connection, 0 otherwise
Mobile	1 if the company uses mobile internet broadband connection, 0 otherwise
Purchase	1 if the company makes purchases of goods or services through internet, 0 otherwise
Gov	1 if the company interacts with government agencies through internet, 0 otherwise

Claims

Average of claims

	Companies
Number of observations	
With advanced security protection	15122
With minimal security protection	1603
Average claims	
With advanced security protection	0.6108
standard deviation	0.0071
With minimal security protection	0.3693
standard deviation	0.0177

Propensity scores and the analysis of self-protection

To begin the analysis, the first step is to calculate propensity scores, which are in this case individual probabilities of acquiring security protection against cyber risk. These probabilities are obtained by estimating a Logit model given by:

$$\widehat{e}(x) = \widehat{\mathbb{P}}(T = 1|x) = \frac{e^{x'\beta}}{1 + e^{x'\beta}}, \tag{1}$$

By estimating propensity scores it is possible to calculate matching estimator that will be done considering a stratified matching.

Propensity scores and the analysis of self-protection

The next step in the analysis is to stratify the data into blocks according to the propensity scores.

A test of balance of each block must be made to guarantee the minimal distance in the marginal distributions of the covariates. We applied the t-test as a balancing test using STATA software.

This test ensures that the means of covariates no differ between the treated and the matched control groups.

A. Azevedo
A. D. Egídio dos Reis
A. I. Bergel

When balance is achieved, the stratified matching can be applied. In this case, the ATT can be expressed as

$$ATT = \sum_{q=1}^{Q} \left(\frac{\sum_{i \in I(q)} Y_i^T}{N_q^T} - \frac{\sum_{j \in I(q)} Y_j^C}{N_q^C} \right) \times \frac{N_q^T}{N^T}, \tag{2}$$

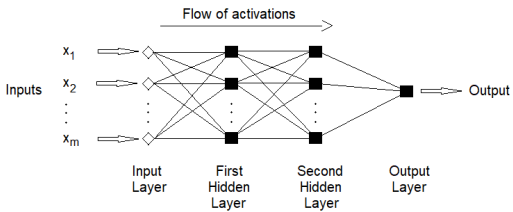
If the result returns a positive value, which in our case was 0.0470, it means that the expected value of number of claims is higher for companies who purchase security protection against cyber risk than for those that do not.

Propensity scores and the analysis of self-protection

As it is a research applied to several companies that individually may have hidden characteristics, therefore not studied, an information asymmetry problem may have resulted into the conclusion that "greater security protection does not imply a lower number of cyber attacks".

A. Azevedo
A. D. Egídio dos Reis
A. I. Bergel

Figure 1: Feedforward multilayer perceptron neural network composed of four layers



Model structure

- The number of nodes in the input layer: 16 explanatory variables;
- The number of hidden layers: Two;
- The number of neurons to be placed in the hidden layers: The first containing 48 neurons and the second 16 neurons;
- The number of neurons in the output layer: The outcome variable, which has a binary character;
- The activation function: Hyperbolic tangent.

Training algorithm

- The most popularly used algorithm for this type of training is the backpropagation algorithm;
- Number of iterations of the algorithm: 6,000;
- Stopping criterion: The estimation of the mean square error below the 0.01 threshold;
- Starting weights, randomly selected in the interval (-0.1, 0.1);
- Learning rate: 0.01;
- The moment term: 0.5.

Confusion matrix

Table 1: Confusion matrix

	Predicted values	
Real values	+	−
+	1847	316
−	273	1744

The proportion of total agreement, that is, the proportion of companies in the test set that were classified as having a claim (non-occurrence), actually presenting a claim (non-occurrence), for the MLP was 86%.

Performance measures

Table 2: Performance measures

	Value
Total error rate	0.14
Total accuracy	0.86
Sensitivity	0.85
Specificity	0.86

- Both the sensitivity and specificity value show that the model proved to be quite efficient in classifying both positive and negative class.

Performance measures *versus* iterations

Figure 2: Performance measures *versus* iterations

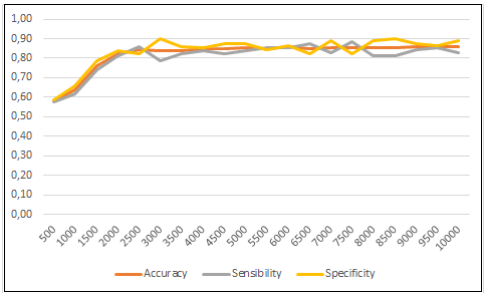
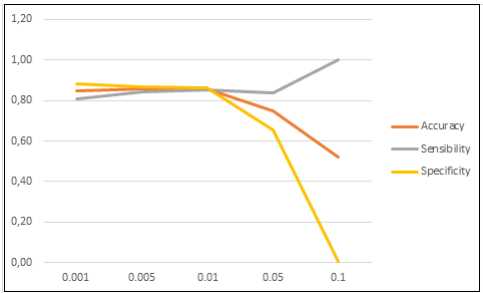


Figure 2 shows the evolution of the values of the performance measures in relation to the increase in the number of iterations.

Performance measures *versus* Learning rate

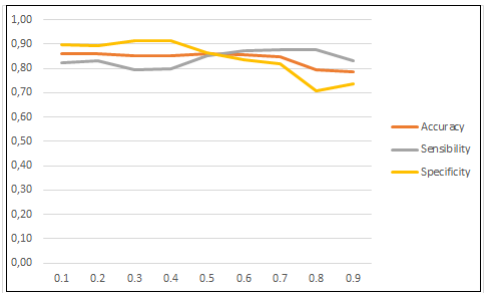
Concerning the variation of the learning rate and the value of the momentum, its influence in the rates of the performance measures was similar.

Figure 3: Performance measures *versus* Learning rate



Performance measures *versus* Momentum

Figure 4: Performance measures *versus* Momentum



Simulations comparison

Table 3: Comparison of the results obtained from the MLP simulations

Classifier	Accuracy	Sensitivity	Specificity
MLP with the best architecture	**0.86**	**0.85**	**0.86**
MLP with three layers and 8 neurons on the hidden layer	0.57	0.45	0.71
MLP similar to the best model but considering logistic activation function	0.82	0.73	0.91
MLP similar to the best model but without momentum	0.86	0.81	0.90

Final Remarks

- Despite informal arguments that favor protection against cyber risks as a tool to improve network security, we observed that in the presence of advanced security protection against cyber risks, the incidence of claims is higher than if a minimal protection existed;
- This result could represent a problem of signaling and screening;

Final Remarks

- The classification results using a MLP neural network trained with a backpropagation algorithm were very good, with 86% global hits;
- The neural model, proposed here, can be conducted in an innovative way as a supporting tool for the decision making of insurers, aiming at useful responses to risk management;

References

Diniz, G.; Muggah, R. & Glenny, M. (2014). Deconstructing cyber security in Brazil: Threats and responses. https://igarape.org.br/wp-content/uploads/en/2014/11/Strategic-Paper-11-Cyber2.pdf.

Gallant, Stephen I & Gallant, Stephen I. (1993). *Neural network learning and expert systems*. MIT press.

Li, M. (2013). Using the propensity score method to estimate causal effects: A review and practical guide. *Organizational Research Methods*, 16(2):188-226.

References

Muggah, Robert & Thompson, Nathan B. (2017). Brazil struggles with effective cyber-crime respons. https://igarape.org.br/brazil-struggles-with-effective-cyber-crime-response/ .

Mukhopadhyay, A.; Chatterjee, S; Saha, D; Mahanti, A. & Sadhukhan, S. K. (2006). e-Risk Management with Insurance: A framework using copula aided bayesian belief networks. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, volume 6, pages 126a-126a.

Ogut, H.; Menon, N. & Raghunathan, S. (2005). Cyber insurance and IT security investment: Impact of interdependent risk. http://infosecon.net/workshop/pdf/56.pdf.

References

Institute, P. (2019). IBM: Cost of a data breach report 2019. https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Repor

Rosenbaum, Paul R. & Rubin, Donald B. (1983). *The central role of the propensity score in observational studies for causal effects*. Biometrika, 70(1):41-55.

Svozil, D.; Kvasnicka, V. & Pospichal, J. (1997). *Introduction to multi-layer feed-forward neural networks*. Chemometrics and Intelligent Laboratory Systems, 39(1):43-62.

Thank you! 

Acknowledgements

The data used in this paper are from the Survey on the use of information and communication technologies in companies, for the year 2010, conducted by "Instituto Brasileiro de Geografia e Estatística" (IBGE), and were obtained through authorized access to the institution's restricted data access room. The results, analyzes and interpretations presented are the sole responsibility of the authors, neither representing the official view of IBGE nor constituting official statistics.

The authors were partially supported by the Project CEMAPRE/REM - UIDB/05069/2020 - financed by FCT/MCTES through national funds.