Cyber Risk Management with Rank-based Statistical Models and Explainable AI

Session 3: Artificial Intelligence for Security in Finance

Paolo Giudici and Emanuela Raffinetti

Department of Economics and Management
University of Pavia (Italy)

14 January 2021

Cyber risk : definition and main concern

Cyber risk :

"any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or the integrity of data or services".

Cybersecurity has become a serious concern for businesses, among operational risks.

Operational risk :

"the risk of a monetary loss caused by human resources, IT systems, by organisation processes or by external events".

While the literature on the quantitative measurement of operational risks, based on loss data, constitutes a reasonably large body, that on cyber risk measurement is very limited. This may be due to the limited availability of data which are typically not disclosed.

Let Y be a response variable, expressed through k ordered categories (severity of cyber attacks).

Procedure :

- assign a rank $r_1 = 1$ to the smallest ordered category of Y ;
- assign rank $(r_{j-1} + n_{j-1})$ to the following ordered categories, where n_{j-1} is the absolute frequency associated with the $(j-1)$-*th* category with $j = 2, \ldots, k$;
- the phenomenon described by the Y variable can be re-formulated in terms of its ranks R, where :

$$R = \left\{ \underbrace{r_1, \ldots, r_1}_{n_1}, \underbrace{r_2, \ldots, r_2}_{n_2}, \ldots, \underbrace{r_k, \ldots, r_k}_{n_k} \right\},$$

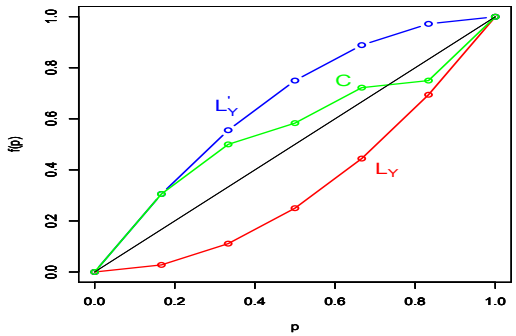
with $r_1 = 1$, $r_2 = r_1 + n_1$ and $r_k = r_{k-1} + n_{k-1}$.

- Given p explanatory variables, a regression model for R can be specified as :

$$\hat{R} = \hat{\beta}_0 + \hat{\beta}_1 X_1 + \hat{\beta}_2 X_2 + \ldots + \hat{\beta}_p X_p,$$

whose unknown parameters can be estimated by the OLS method.

To validate the model, we resort to a recently developed criterion called *Rank Graduation Accuracy* (*RGA*), which is based on the Lorenz (L_Y), dual Lorenz ($L_Y^{'}$) and concordance (C) curves.



Being $Y = R$, the *RGA* index is defined as :

$$RGA = \sum_{i=1}^{n} \frac{\left\{ (1/(n\bar{r})) \sum_{j=1}^{i} r_{ord(\hat{r}_j)} - i/n \right\}^2}{i/n} = \sum_{i=1}^{n} \frac{\left\{ C(r_{ord(\hat{r}_j)}) - i/n \right\}^2}{i/n}$$

where $r_{ord(\hat{r}_j)}$ are the rank-transformed response variable values, re-ordered by the ranks predicted by the model, $\bar{r}$ is the mean of all ranks and $C(r_{ord(\hat{r}_j)}) = \frac{\sum_{j=1}^{i} r_{ord(\hat{r}_j)}}{\sum_{i=1}^{n} r_{ord(r_i)}}$.
RGA_{norm} can be specified as the ratio between *RGA* and its maximum value ($RGA_{norm} \in [0, 1]$).

The test statistics is formalized as :

$$T = \sum_{i=1}^{n} \frac{\left\{ \sum_{j=1}^{i} R_{ord(\hat{r}_j)} - \sum_{j=1}^{i} R^e_{ord(\hat{r}_j)} \right\}^2}{\sum_{j=1}^{i} R^e_{ord(\hat{r}_j)}},$$

where $R^e_{ord(\hat{r}_j)}$ is the expected rank-transformed response variable value in the case of a random model and $T \sim \chi^2_n$.

The comparison may occur between a full model (including all the covariates in the dataset) and a reduced model (including only some of the covariates in the dataset).

- Define with T_{full} the test statistics T computed under the full model.
- Define with $T_{reduced}$ the same statistics computed under the reduced model.
- Let $T_{model} = T_{full} - T_{reduced}$ be the difference between the two test statistics.
- The following proposition holds :

Proposition. $T_{model} = T_{full} - T_{reduced}$ is distributed as a Variance Gamma distribution, with parameters $\lambda = n/2$, $\alpha = 1/2$, $\beta = 0$ and $\mu = 0$, where λ and $\alpha \in \mathbb{R}$, β is the asymmetry parameter and μ is the location parameter.

If we resort to the VarianceGamma R package, the parameter λ must be set equal to one half the number of observations included in the dataset. But the computation of the *p*-values of the VarianceGamma associated with the R package is not possible when λ takes large values.

A possible solution is to focus only on samples of small size which may be directly drawn by the dataset.

To overcome this problem we refer to the subsampling procedure introduced by Raffinetti and Romeo (2015).

- Consider a number h of different samples and compute for each sample the value of the test T_{model}.
- The Variance Gamma distribution is symmetric around zero. This consideration, suggests the use of a bilateral test.

A *significance value* (named *s*-value) defined as the relative percentage of significant tests

$$s\text{-value} = P(T_{imodel} \geq |t_{\alpha/2}|) = \frac{1}{h}\sum_{i=1}^{h} I_{T_{imodel} \geq |t_{\alpha/2}|}, \quad i = 1, \ldots, h,$$

where

$$I_{T_{imodel} \geq |t_{\alpha/2}|} = \begin{cases} 0, \text{ if } -t_{\alpha/2} < T_{imodel} < t_{\alpha/2} \\ 1, \text{ otherwise.} \end{cases}$$

is employed.

The *s*-value can be associated with a significance scale (*s*-scale) summarised as follows :

s-value classes	*s*-classes levels
s-value=1	Always significant
0.7$<$*s*-value$<$1	Almost always significant
0.5$<$*s*-value$\leq$0.7	Frequently significant
0.3$<$*s*-value$\leq$0.5	Sometimes significant
0$<$*s*-value$\leq$0.3	Rarely significant
s-value=0	Never significant

Data

Our proposal is applied to real loss data, organised by severeity levels, reported in the italian annual report on cyber risks (Clusit, 2018).

We focus on a sample data, consisting of 808 cyber attacks observed in 2017.

Severity levels are reported according to the type and technique of attacks (which can be seen as event types), the victims and their country of origin (which can be seen as business lines).

Analysis

The aim is to detect the main factors which may affect the severity degree. We consider three rank regression models which differ in terms of the variables taken into account :

- the first rank regression model is built on all the explanatory variables appearing in our dataset (cyber attacks, attack techniques, victim type and continent) ;
- the second rank regression model was specified by removing from the full model the continent variable, in order to assess if the geographical area where the cyber attacks occur may impact on the severity degree ;
- the third rank regression model was built by removing from the full model the cyber attack type variable.

Results

	Full model		Reduced model (without continent variable)	
Coefficient	***Estimate***	***p-value***	***Estimate***	***p-value***
Intercept	87.42	0.02678	175.65	0.01615
Espionage/Sabotage	-231.38	$<$0.001	-231.88	$<$0.001
Hacktivism	-39.210	0.00663	-38.99	0.00672
Information warfare	-222.17	$<$0.001	-221.71	$<$0.001
Entertainment/News	117.14	0.03345	115.53	0.03549
GDO/Retail	139.97	0.01743	138.18	0.01855
Online Services/Cloud	136.11	0.01496	135.52	0.01514
Research-Education	142.26	0.01057	140.07	0.01158
Phishing/Social Engineering	120.27	0.01763	120.63	0.01708
Unknown	99.670	0.04516	100.21	0.04357

Categorical variable reference level : cyber attack (first block) : Cybercrime ; victim type (second block) : Automotive ; attack technique (third block) : 0-day

Remark :

In the reduced rank regression model **without the cyber attack variable**, Entertainment/News is no more significant while DDoS, Malware, Malware and Vulnerabilities become significant.

Model	*RGA*	RGA_{norm}	RMSE
Full rank regression model	63.185	0.739	105.196
Reduced rank regression model (without continent variable)	63.111	0.738	105.284
Reduced rank regression model (without cyber attack variable)	47.426	0.555	122.706

Testing the additional contribution

The assessment of the significance in the difference between the full model and the reduced model without the cyber attack is led by resorting to the subsampling procedure proposed by Raffinetti and Romeo (2015).

We specify :

- $\alpha = 0.05$, as significance level ;
- n=10, as the sample size ;
- $h = \{100, 500, 1,000\}$, as the number of samples drawn from the dataset.

h	s-value	s-scale
100	0.750	Almost always significant
500	0.788	Almost always significant
1,000	0.811	Almost always significant

The Shapley-Lorenz decomposition

The Shapley-Lorenz decomposition appears as new eXplainable Artificial Intelligence method and can be expressed as :

$$LZ_{d=1}^{X_k}(\hat{Y}) = \sum_{X' \subseteq \mathcal{C}(X) \setminus X_K} \frac{|X'|!(K - |X'| - 1)!}{K!} [LZ(\hat{Y}_{X' \cup X_k}) - LZ(\hat{Y}_{X'})],$$

where $LZ(\hat{Y}_{X' \cup X_k})$ and $LZ(\hat{Y}_{X'})$ describe the (mutual) variability explained by the models including the $X' \cup X_k$ variables and the X' variables, respectively.

Results

Additional covariate (X_k)	$LZ_{d=1}^{X_k}(\widehat{Severity})$	Global Shapley
Type of attack	0.072	-748.96
Type of victim	0.115	5.15
Technique of attack	0.058	-34.36
Continent	0.032	-25.67

Some basic references

Afful-Dadzie, A. and Allen, T.T. (2017), “Data-Driven Cyber-Vulnerability Maintenance Policies”, Journal of Quality Technology, Vol. 46 No. 3, pp. 234-250.

Alexander, C. (2003), Operational risk : regulation, analysis and management, Prentice Hall, New York, NY.

Clusit (2018), “2018 Report on ICT security in Italy”.

Cruz, M. (2002), Modeling, measuring and hedging operational risk, Wiley, New York, NY.

Edgar, T.W. and Manz, D.O. (2017), Research Methods for Cyber Security, Elsevier.

Giudici, P. and Bilotta, A. (2004), “Modelling operational losses : a Bayesian approach”, Quality and reliability Engineering International, Vol. 20 No. 5, pp. 407-417.

Agosto, A., Giudici, P. and Raffinetti, E. (2019), “A Rank-based method to improve the predictive accuracy measurement of credit ratings”, Technical report, submitted.

Hubbard, D.W. and Seiersen, R. (2016), How to Measure Anything in Cybersecurity Risk, Wiley, New York, NY.

Kopp, E., Kaffenberger, L. and Wilson, C. (2017), “Cyber Risk, Market Failures, and Financial Stability”, IMF Working Paper, WP/17/185, pp. 1-35.

Koshevoy, G. and Mosler, K (1996), “The Lorenz Zonoid of a Multivariate Distribution”, Journal of the American Statistical Association, Vol. 91 No. 434, pp. 873-882.

Raffinetti, E. and Romeo, I. (2015), “Dealing with the biased effects issue when handling huge datasets : the case of INVALSI data”, Journal of Applied Statistics, Vol. 42 No. 12, pp. 2554-2570.

Scott, D. and Yang Dong, C. (2018), “R package VarianceGamma”.

Seneta, E. (2004), “Fitting the variance-gamma model to financial data”, Journal of Applied Probability, Vol. 41 No. A, pp. 177-187.

Shapley, L..S. (1953), “A value for *n*-person games”, Contributions to the Theory of Games, 307-317.