USE CASE
Cyber risk ordering with rank-based statistical models and eXplainaible Artificial Intelligence methods

Emanuela Raffinetti and Paolo Giudici

University of Pavia (Italy)

18 June, 2021

Cyber risk : definition, main concerns and proposals

Definition

Cyber risk may be intended as any risk emerging from intentional attacks on information and communication technology (ICT) systems that compromises the confidentiality, availability, or the integrity of data or services.

Main concerns

- Lack in the availability of monetary loss data, which are typically not disclosed. When disclosed, they are often expressed in terms of ordered levels of severity, such as “low”, “medium” or “high” severity.
- The use of Artificial Intelligence (AI) methods may be not suitable due to their black box nature.

Proposals

- Predicting the ordinal severity levels of cyber risks with a methodology based on rank regression models.
- Providing a new global eXplainable AI method, based on the Shapley-value approach and the Lorenz tool (Shapley Lorenz decomposition), aimed at detecting the main factors impacting on the cyber attack severity.

Data and methodology

Data

- Real loss data, organised by severity levels, reported in the italian annual report on cyber risks (Clusit, 2018).
- 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, the victims and their country of origin.

Methodology

Let Y represent the severity of cyber attacks, expressed through h ordered categories.

- The Y variable can be re-formulated in terms of its ranks R, where
  $R = \left\{ \underbrace{r_1, \ldots, r_1}_{n_1}, \underbrace{r_2, \ldots, r_2}_{n_2}, \ldots, \underbrace{r_h, \ldots, r_h}_{n_h} \right\}$, with $r_1 = 1$ and $r_j = r_{j-1} + n_{j-1}$, for $j = 2, \ldots, h$.
- Given K explanatory variables :
  1) a regression model for R is specified as $\hat{R} = \hat{\beta}_0 + \hat{\beta}_1 X_1 + \hat{\beta}_2 X_2 + \ldots + \hat{\beta}_K X_K$;
  2) the marginal contribution of the additional variable $X_k, (k = 1, \ldots, K)$ can be expressed as $LZ^{X_k}(\hat{R}) = \sum_{X' \subseteq \mathcal{C}(X) \setminus X_k} \frac{|X'|!(K-|X'|-1)!}{K!} [LZ(\hat{R}_{X' \cup X_k}) - LZ(\hat{R}_{X'})]$, where $LZ(\hat{R}_{X' \cup X_k})$ and $LZ(\hat{R}_{X'})$ describe the (mutual) variability explained by the models including the $X' \cup X_k$ variables and the X' variables.

Results - Rank Regression Model & Shapley Lorenz decomposition

	Full model	
Coefficient	***Estimate***	***p-value***
Intercept	187.42	0.02678
Espionage/Sabotage	-231.38	$<$0.001
Hacktivism	-39.210	0.00663
Information warfare	-222.17	$<$0.001
Entertainment/News	117.14	0.03345
GDO/Retail	139.97	0.01743
Online Services/Cloud	136.11	0.01496
Research-Education	142.26	0.01057
Phishing/Social Engineering	120.27	0.01763
Unknown	99.670	0.04516

Additional covariate (X_k)	$LZ^{X_k}(\widehat{Severity})$
Type of attacker	0.072
Type of victim	0.115
Technique of attack	0.058
Continent	0.032

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

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.

Cebula, J.J. and Young, L.R. (2010), “A Taxonomy of Operational Cyber Security Risks”, Technical Note, CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, pp. 1-34.

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.

Giudici P. and Raffinetti E. (2020), “Cyber risk ordering with rank-based statistical models”, AStA Advances in Statistical Analysis (2020).

Giudici P. and Raffinetti E. (2021), “Explainable AI methods in cyber risk management”, Quality and Reliability Engineering International.

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.

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